Ernst & Young P/S
Osvald Helmuths Vej 4
P.O. Box 250
2000 Frederiksberg
Denmark

Telephone +45 73 23 30 00
Telefax +45 72 29 30 30
www.ey.com/dk
Reg. no. 30 70 02 28

Independent Assurance Report

To the management of Telia Company AB (Telia):

Scope

We have been engaged, in a reasonable assurance engagement, to report on Telia management's statement that, except for matters described in the statement, for its Certification Authority (CA) operations in Finland and Sweden, throughout the period 1 April 2017 through 31 March 2018 for its CAs as enumerated in Attachment A, Telia has:

- disclosed its SSL certificate life cycle management business practices in its:
  - Telia Root Certificate Policy and Certification Practice Statement v2.2;
  - Telia Server Certificate Policy and Certification Practice Statement v2.1;
  - Telia Gateway Certificate Policy and Certification Practice Statement v1.5;
  - Telia Organizational User Certificate Policy and Certification Practice Statement v1.3;
  - TeliaSonera Customer CA Certificate Policy and Certification Practice Statement v1.2; and
  - Telia Production Certification Practice Statement v2.5

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Telia website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that
  - the integrity of keys and SSL certificates it manages is established and protected throughout their life cycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by Telia)
- maintained effective controls to provide reasonable assurance that
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

And, for its CAs as enumerated in Attachment A

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2.

Certification Authority's responsibilities

Telia's management is responsible for its statement, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2.

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Ernst & Young Godkendt Revisionspartnerselskab applies International Standard on Quality Control 1[1] and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on management's statement based on our procedures. We conducted our procedures in accordance with International Standards on Assurance Engagements 3000 *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's statement is fairly stated, and, accordingly, included:

(1) obtaining an understanding of Telia's SSL certificate life cycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of Telia's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;

(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.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at Telia 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.

Inherent limitations

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

Basis for qualified opinion

During our procedures, we noted the following that caused a qualification of our opinion:

[1] ISQC 1, Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements

#	Deviation	Relevant WebTrust Criteria
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.
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.
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.
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 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.	**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 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 …
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 …

#	Deviation	Relevant WebTrust Criteria
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.
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.
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.
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.

Qualified Opinion

In our opinion, except for the matters described in the basis for qualified opinion section above, throughout the period 1 April 2017 to 31 March 2018, Telia has, in all material respects:

- disclosed its SSL certificate life cycle management business practices in its:
  - Telia Root Certificate Policy and Certification Practice Statement v2.2;
  - Telia Server Certificate Policy and Certification Practice Statement v2.1;
  - Telia Gateway Certificate Policy and Certification Practice Statement v1.5;
  - Telia Organizational User Certificate Policy and Certification Practice Statement v1.3;
  - TeliaSonera Customer CA Certificate Policy and Certification Practice Statement v1.2; and
  - Telia Production Certification Practice Statement v2.5

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Telia website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that
  - the integrity of keys and SSL certificates it manages is established and protected throughout their life cycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by Telia)
- maintained effective controls to provide reasonable assurance that
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2.

This report does not include any representation as to the quality of Telia's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, nor the suitability of any of these Telia's services for any customer's intended purpose.

Copenhagen June 29, 2018

Ernst & Young P/S
Godkendt Revisionspartnerselskab

Claus Thaudahl Hansen
Partner, State Authorised Public Accountant
MNE no 19675

Juha Sunila
Senior Manager, CISA, CISSP

Attachment A: List of CAs in Scope

The following CAs were in scope for the SSL Baseline Requirements and Network Security Requirements:

CA #	Cert. #	Subject	Issuer	Serial	Key Algorithm and Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA1 Fingerprint	Other information
1	1	CN = Sonera Class2 CA O = Sonera C = FI	Self-signed	1d	RSA 2048 bits	sha1RSA	6 April 2001	6 April 2021	4a a0 aa 58 84 d3 5e 3c	37 f7 6d e6 07 7c 90 c5 b1 3e 93 1a b7 41 10 b4 f2 e4 9a 27	
2	1	CN = TeliaSonera Root CA v1 O = TeliaSonera	Self-signed	00 95 be 16 a0 f7 2e 46 f1 7b 39 82 72 fa 8b cd 96	RSA 4096 bits	sha1RSA	18 October 2007	18 October 2032	f0 8f 59 38 00 b3 f5 8f 9a 96 0c d5 eb fa 7b aa 17 e8 13 12	43 13 bb 96 f1 d5 86 9b c1 4e 6a 92 f6 cf f6 34 69 87 82 37	
	2	CN = TeliaSonera Root CA v1 O = TeliaSonera	Sonera Class2 CA	00 87 ed 2e 1a 28 26 4a c5 19 aa 3a eb b9 0d a2 cb	RSA 4096 bits	sha256RSA	5 December 2014	5 April 2021	f0 8f 59 38 00 b3 f5 8f 9a 96 0c d5 eb fa 7b aa 17 e8 13 12	9f f6 1d eb b4 ed 26 3b 4d be c7 79 87 ca 49 3c 6c c9 3a a4	
	3	CN = TeliaSonera Root CA v1 O = TeliaSonera	Sonera Class2 CA	00 d1 e0 3e 5b 48 ed c7 9e 09 3f 40 de e1 61 c3 8b	RSA 4096 bits	sha1RSA	18 October 2007	17 October 2019	f0 8f 59 38 00 b3 f5 8f 9a 96 0c d5 eb fa 7b aa 17 e8 13 12	f4 67 16 7f 48 8b c8 34 66 38 88 a6 9a db 4c b9 74 16 d6 06	
3	1	CN = TeliaSonera Extended Validation SSL CA v1 O = TeliaSonera C = FI	TeliaSonera Root CA v1	00 99 38 b8 d6 06 28 ea 59 2e 26 01 0f d2 66 e8 11	RSA 4096 bits	sha256RSA	16 March 2015	17 October 2032	08 e4 fa 72 d5 43 3b c2 5c 24 9b 95 92 40 f3 d0 9f 7a a8 30	f1 f5 48 b0 1e b2 66 fa 95 c3 0f 79 c3 c9 1f 58 ea 3d f1 8c	
4	1	CN = TeliaSonera Server CA v2 O = TeliaSonera C = FI	TeliaSonera Root CA v1	4c 46 2a f6 db fb f7 80 4f 84 c1 7c fe a9 72 b6	RSA 4096 bits	sha256RSA	16 October 2014	16 October 2032	2f 49 3c 29 4f d7 07 25 f9 c6 8c d5 64 f5 66 3d 12 83 22 95	0e c6 42 d0 0f 8d cf 7b 19 6a c0 a9 f2 c8 57 e3 42 68 79 a4	
5	1	CN = TeliaSonera Server CA v1 O = TeliaSonera	TeliaSonera Root CA v1	10 68 4a 0d 86 e8 43 59 2d 16 74 6a 88 15 2f 81	RSA 4096 bits	sha1RSA	13 May 2013	17 October 2032	a0 81 be 55 9b f3 7f 61 05 84 8b 2d 0c 3b e0 08 49 ee 57 3e	41 c4 34 fa 80 ed b4 bf 58 a6 98 c2 b1 54 20 d6 f3 4a 33 d0	The CA did not issue certificates during the period 1 Apr 2017 to 31 Mar 2018 and was maintained online to provide revocation status information only.
6	1	CN = TeliaSonera Gateway CA v2 O = TeliaSonera C = FI	TeliaSonera Root CA v1	00 86 3c 75 64 11 95 85 4f b4 31 38 a0 a0 cf 8a a3	RSA 4096 bits	sha256RSA	16 October 2014	16 October 2032	87 aa e3 13 12 9f 11 8b ca 68 cd 1e 2d c4 29 a8 fa 10 1a cb	3f 1a 1c cb eb b8 c7 3b e9 94 46 91 8e 3f af f3 ae d2 47 a3	

CA #	Cert. #	Subject	Issuer	Serial	Key Algorithm and Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA1 Fingerprint	Other information
7	1	CN = TeliaSonera Gateway CA v1 O = TeliaSonera	TeliaSonera Root CA v1	35 79 1d 87 92 51 6d 61 b1 1c 4b ef af 76 c1 da	RSA 4096 bits	sha1RSA	13 May 2013	17 October 2032	8f 59 95 28 26 a2 b0 6d 19 49 99 d2 fb b0 84 47 4d cb 95 fc	0d e2 60 f7 96 5c c7 d1 cc be 92 21 26 68 52 9f e5 5f 7d cd	The CA did not issue certificates during the period 1 Apr 2017 to 31 Mar 2018 and was maintained online to provide revocation status information only.
8	1	CN = Telia Domain Validation SSL CA v1 O = Telia Finland Oyj C = FI	TeliaSonera Root CA v1	01 61 ae 20 05 ce 3f 12 7e f8 8d d7 25 1b b1	RSA 4096 bits	sha256RSA	19 February 2018	16 October 2032	49 6c 32 53 7c 5d ed 2b e3 a2 ab 9c 0b c9 5d e4 95 d4 92 5f	8e 16 4d f8 80 51 da 37 8a 68 d8 f4 01 87 6d 29 c1 c7 7c 5b	

The following CAs have not issued publicly trusted SSL/TLS certificates intended to authenticate servers on the Internet (i.e. certificates containing the id-kp-serverAuth OID (1.3.6.1.5.5.7.3.1) in the extendedKeyUsage extension) and they were in scope only for the Network Security Requirements:

CA #	Cert. #	Subject	Issuer	Serial	Key Algorithm and Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA1 Fingerprint	Other information
9	1	CN = Telia Document Signing CA v1 O = Telia Finland Oyj C = FI	TeliaSonera Root CA v1	01 60 4b 22 f6 76 3f 09 01 ee 04 83 6b 97 3c	RSA 4096 bits	sha256RSA	28 November 2017	18 October 2032	ee 2a a3 20 42 d6 99 4e 4e 3d 1e 9e 4f e0 b8 a9 9d 74 db fa	59 51 61 ab 72 81 54 58 76 bf 38 ad 93 6c c0 3a b1 2b 8f 90	
10	1	CN = TeliaSonera Class 1 CA v2 O = TeliaSonera C = FI	TeliaSonera Root CA v1	00 fd 41 dd 7f d1 9f 3e e9 f8 5d 9e 43 71 33 d4 db	RSA 4096 bits	sha256RSA	16 October 2014	16 October 2032	d1 47 22 8f cb a8 5d 1a fe 26 41 46 6e cb 82 4b 65 7d 8a e4	89 e3 c8 68 96 af 10 e2 f4 ee cb c8 12 04 6e b9 a4 4c 8f d0	
11	1	CN = TeliaSonera Class 1 CA v1 O = TeliaSonera	TeliaSonera Root CA v1	00 f8 5d 2f 19 0c 60 9f 14 94 b2 8d f9 c1 d1 e7 4c	RSA 4096 bits	sha1RSA	13 May 2013	17 October 2032	f5 ea 33 8c f8 a5 2e 8c a6 82 6b 4d 8b 32 2a a7 b7 53 cf cc	6c 0d 9c 40 94 9c 7e a5 72 a5 b9 48 01 98 8a 9f 19 b4 07 e9	The CA did not issue certificates during the period 1 Apr 2017 to 31 Mar 2018 and was maintained online to provide revocation status information only.
12	1	CN = TeliaSonera Class 2 CA v2 O = TeliaSonera C = SE	TeliaSonera Root CA v1	63 7c 0b d7 85 a5 bf 29 da 60 2d 7c 4d 7a 70 b1	RSA 4096 bits	sha256RSA	16 October 2014	16 October 2032	9e 19 ff e5 0d 3a fe 00 97 15 3f 69 f1 dc 5a 3c aa 0c 94 83	25 5a d6 e3 86 59 63 cf 5a d9 7b 31 2a 26 86 e2 4e db 92 24	

CA #	Cert. #	Subject	Issuer	Serial	Key Algorithm and Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA1 Fingerprint	Other information
13	1	CN = TeliaSonera Class 2 CA v1 O = TeliaSonera	TeliaSonera Root CA v1	00 d0 d7 72 72 9a 04 17 97 f8 9e da e3 82 f9 1f 11	RSA 4096 bits	sha1RSA	13 May 2013	17 October 2032	d4 6d bd b2 55 bb 52 4b 2a e8 b3 df 6d a7 d8 01 fb 67 9f 72	51 e6 35 0e 44 5c 1f 7c ca a2 7d 5b 6b a2 1d 28 65 ae 04 a4	
14	1	CN = TeliaSonera Email CA v4 O = TeliaSonera C = SE	TeliaSonera Root CA v1	52 eb a0 d8 b7 4b 46 eb 85 57 cd 6d a2 a3 dd dd	RSA 4096 bits	sha256RSA	16 October 2014	16 October 2032	89 86 2a 82 d1 78 fa f0 a6 29 54 35 87 95 6f d3 77 60 19 f0	df fd 4e 47 cf f7 c0 17 0a 53 eb ea 18 20 fb 4f 95 04 60 f5	
15	1	CN = TeliaSonera Email CA v3 O = TeliaSonera	TeliaSonera Root CA v1	00 81 51 ad 72 8b 67 a5 7f a4 55 24 8d 81 d3 57 f9	RSA 4096 bits	sha1RSA	13 May 2013	17 October 2032	f3 74 b8 1d 13 33 d1 c9 ad 5b ce 66 28 9a 99 32 81 f0 20 ce	11 ef 59 16 40 5e 41 0d 0e c7 45 36 f9 f1 90 f6 ed 62 96 29	The CA did not issue certificates during the period 1 Apr 2017 to 31 Mar 2018 and was maintained online to provide revocation status information only.
16	1	CN = Ericsson NL Individual CA v3 O = Ericsson C = SE	TeliaSonera Root CA v1	53 b8 7e 83 e1 9c 99 28 93 b0 9b 49 1c ec b8 eb	RSA 4096 bits	sha256RSA	27 October 2015	27 October 2025	1c 7b 19 9e 97 9c 76 ac 20 3d d8 dc e3 91 6a e3 db 2d a6 53	f5 d9 4b dd 46 fe 6f 7b 3b 29 d0 b0 a4 37 fd 47 96 65 4d e5	The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-emailProtection
17	1	CN = Ericsson NL Individual CA v2 O = Ericsson	TeliaSonera Root CA v1	00 a0 0c cb cc 9b 99 98 ec e2 3a 70 f4 7c c1 c0 59	RSA 4096 bits	sha1RSA	27 May 2014	27 May 2024	b1 0d ca d4 46 b7 af 86 02 c3 2f 6f 06 ca 0e 76 71 7f 4b 37	27 45 1f a5 c9 1d aa bf e4 2e b1 e5 49 07 df 32 a5 b1 58 b0	The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-emailProtection

The following CAs in the CA hierarchy were not in the scope of the engagement. According to the CA, they have not issued publicly distributed and trusted certificates, instead the certificates are only relied by Telia's authentication service.

CA #	Cert. #	Subject	Issuer	Serial	Key Algorithm and Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA1 Fingerprint	Other information
18	1	CN = TeliaSonera Mobile ID CA v2 O = TeliaSonera Finland Oyj C = FI	TeliaSonera Root CA v1	01 61 ae 3e 89 33 e5 b8 95 8a ef 92 9c 0c eb	RSA 4096 bits	sha256RSA	19 February 2018	17 October 2032	d0 2d d3 14 f0 77 4a 62 27 2c 65 53 93 d5 a5 a5 43 af c2 52	16 6a 7f a3 7f eb 9f 97 87 ea b2 69 88 a0 98 ca 27 ae 04 0b	The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-timeStamping
	2	CN = TeliaSonera Mobile ID CA v2 O = TeliaSonera Finland Oyj C = FI	TeliaSonera Root CA v1	03 75 c4 9b 7e 63 ce 43 37 07 ff 19 84 37 a5 ef	RSA 4096 bits	sha256RSA	26 January 2016	17 October 2032	d0 2d d3 14 f0 77 4a 62 27 2c 65 53 93 d5 a5 a5 43 af c2 52	57 b2 20 23 1d c6 b6 9c a5 0a cc c9 bc 66 b0 84 9b aa 78 2a	The certificate has been revoked 17 Apr 2018. The CA certificate had the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-emailProtection id-kp-timeStamping
19	1	CN = TeliaSonera Mobile ID CA v1 O = TeliaSonera Finland Oyj C = FI	TeliaSonera Root CA v1	01 63 8b ea 73 4a fa f8 7f 6e 51 24 37 1f 72	RSA 4096 bits	sha256RSA	23 May 2018	16 October 2032	53 80 2c e5 18 4b 1e c1 0b d6 26 2c d1 08 ef 88 86 dd 2c 0e	68 a5 35 9c a1 c7 72 33 ca 27 66 3f 1d 29 7e e8 43 62 a1 22	The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth
	2	CN = TeliaSonera Mobile ID CA v1 O = Telia Finland Oyj C = FI	TeliaSonera Root CA v1	01 62 af 14 90 9a 4c 15 5a 56 ba 6d b7 ab 5f	RSA 4096 bits	sha256RSA	10 April 2018	16 October 2032	53 80 2c e5 18 4b 1e c1 0b d6 26 2c d1 08 ef 88 86 dd 2c 0e	90 ef e8 0c da 70 af 07 10 93 8f c6 a9 d0 60 9c 0c f4 4a ba	The certificate has been revoked 23 May 2018. The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth
	3	CN = TeliaSonera Mobile ID CA v1 O = TeliaSonera Finland Oyj C = FI	TeliaSonera Root CA v1	00 d7 6a 8b c5 05 09 00 a1 9b 44 5c 87 28 cc a6 36	RSA 4096 bits	sha256RSA	16 October 2014	16 October 2032	53 80 2c e5 18 4b 1e c1 0b d6 26 2c d1 08 ef 88 86 dd 2c 0e	80 2f f3 0f b8 b6 26 63 35 c2 fc a8 6e 20 c3 df ff fd 6a 19	The certificate has been revoked 17 Apr 2018. The CA certificate had the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-emailProtection
	4	CN = TeliaSonera Mobile ID CA v1 O = TeliaSonera Finland Oyj C = FI	TeliaSonera Root CA v1	00 f9 4c 94 77 c4 fb 88 be 33 5e 65 72 d3 7a 72 25	RSA 4096 bits	sha256RSA	16 December 2010	17 October 2032	53 80 2c e5 18 4b 1e c1 0b d6 26 2c d1 08 ef 88 86 dd 2c 0e	cb 18 ac 54 e8 d1 6c 01 93 dd 95 4e 18 53 7b 8a 71 b2 34 e7	

TELIA'S MANAGEMENT STATEMENT

Telia Company AB (Telia) operates the Certification Authority (CA) services as enumerated in Attachment A, and provides SSL CA services.

Telia management has assessed its disclosures of its certificate practices and controls over its SSL CA services. During our assessment we noted the following deviations which caused the relevant criteria to not be met:

#	Deviation	Relevant WebTrust Criteria
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.
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.
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.
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 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.	**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 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 … …
5	Many organization validated subscriber certificates included an email address as an optional subject attribute in the Subject field of the certificate and the	**Principle 2, Criterion 2.14**

#	Deviation	Relevant WebTrust Criteria
	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.	The CA maintains controls to provide reasonable assurance that Subject information of Certificates conforms to the Baseline Requirements, including: … • Other Subject Attributes …
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.
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.
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.
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.

Based on that assessment, in Telia management's opinion, except for the matters described in the

preceding table, in providing its SSL and non-SSL Certification Authority (CA) services in Finland and Sweden, throughout the period 1 April 2017 to 31 March 31 2018, Telia has:

- disclosed its SSL certificate life cycle management business practices in its:
  - Telia Root Certificate Policy and Certification Practice Statement v2.2;
  - Telia Server Certificate Policy and Certification Practice Statement v2.1;
  - Telia Gateway Certificate Policy and Certification Practice Statement v1.5;
  - Telia Organizational User Certificate Policy and Certification Practice Statement v1.3;
  - TeliaSonera Customer CA Certificate Policy and Certification Practice Statement v1.2; and
  - Telia Production Certification Practice Statement v2.5

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Telia website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that
  - the integrity of keys and SSL certificates it manages is established and protected throughout their life cycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by Telia)
- maintained effective controls to provide reasonable assurance that
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2.

Stockholm, 29 June 2018

Telia Company AB

Shahryar Khan
Head of GSO NW Transport Automation and Systems

Attachment A: List of CAs in Scope

The following CAs were in scope for the SSL Baseline Requirements and Network Security Requirements:

CA #	Cert. #	Subject	Issuer	Serial	Key Algorithm and Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA1 Fingerprint	Extended Key Usage
1	1	CN = Sonera Class2 CA O = Sonera C = FI	Self-signed	1d	RSA 2048 bits	sha1RSA	6 April 2001	6 April 2021	4a a0 aa 58 84 d3 5e 3c	37 f7 6d e6 07 7c 90 c5 b1 3e 93 1a b7 41 10 b4 f2 e4 9a 27	
2	1	CN = TeliaSonera Root CA v1 O = TeliaSonera	Self-signed	00 95 be 16 a0 f7 2e 46 f1 7b 39 82 72 fa 8b cd 96	RSA 4096 bits	sha1RSA	18 October 2007	18 October 2032	f0 8f 59 38 00 b3 f5 8f 9a 96 0c d5 eb fa 7b aa 17 e8 13 12	43 13 bb 96 f1 d5 86 9b c1 4e 6a 92 f6 cf f6 34 69 87 82 37	
	2	CN = TeliaSonera Root CA v1 O = TeliaSonera	Sonera Class2 CA	00 87 ed 2e 1a 28 26 4a c5 19 aa 3a eb b9 0d a2 cb	RSA 4096 bits	sha256RSA	5 December 2014	5 April 2021	f0 8f 59 38 00 b3 f5 8f 9a 96 0c d5 eb fa 7b aa 17 e8 13 12	9f f6 1d eb b4 ed 26 3b 4d be c7 79 87 ca 49 3c 6c c9 3a a4	
	3	CN = TeliaSonera Root CA v1 O = TeliaSonera	Sonera Class2 CA	00 d1 e0 3e 5b 48 ed c7 9e 09 3f 40 de e1 61 c3 8b	RSA 4096 bits	sha1RSA	18 October 2007	17 October 2019	f0 8f 59 38 00 b3 f5 8f 9a 96 0c d5 eb fa 7b aa 17 e8 13 12	f4 67 16 7f 48 8b c8 34 66 38 88 a6 9a db 4c b9 74 16 d6 06	
3	1	CN = TeliaSonera Extended Validation SSL CA v1 O = TeliaSonera C = FI	TeliaSonera Root CA v1	00 99 38 b8 d6 06 28 ea 59 2e 26 01 0f d2 66 e8 11	RSA 4096 bits	sha256RSA	16 March 2015	17 October 2032	08 e4 fa 72 d5 43 3b c2 5c 24 9b 95 92 40 f3 d0 9f 7a a8 30	f1 f5 48 b0 1e b2 66 fa 95 c3 0f 79 c3 c9 1f 58 ea 3d f1 8c	
4	1	CN = TeliaSonera Server CA v2 O = TeliaSonera C = FI	TeliaSonera Root CA v1	4c 46 2a f6 db fb f7 80 4f 84 c1 7c fe a9 72 b6	RSA 4096 bits	sha256RSA	16 October 2014	16 October 2032	2f 49 3c 29 4f d7 07 25 f9 c6 8c d5 64 f5 66 3d 12 83 22 95	0e c6 42 d0 0f 8d cf 7b 19 6a c0 a9 f2 c8 57 e3 42 68 79 a4	
5	1	CN = TeliaSonera Server CA v1 O = TeliaSonera	TeliaSonera Root CA v1	10 68 4a 0d 86 e8 43 59 2d 16 74 6a 88 15 2f 81	RSA 4096 bits	sha1RSA	13 May 2013	17 October 2032	a0 81 be 55 9b f3 7f 61 05 84 8b 2d 0c 3b e0 08 49 ee 57 3e	41 c4 34 fa 80 ed b4 bf 58 a6 98 c2 b1 54 20 d6 f3 4a 33 d0	The CA did not issue certificates during the period 1 Apr 2017 to 31 Mar 2018 and was maintained online to provide revocation status information only.
6	1	CN = TeliaSonera Gateway CA v2 O = TeliaSonera C = FI	TeliaSonera Root CA v1	00 86 3c 75 64 11 95 85 4f b4 31 38 a0 a0 cf 8a a3	RSA 4096 bits	sha256RSA	16 October 2014	16 October 2032	87 aa e3 13 12 9f 11 8b ca 68 cd 1e 2d c4 29 a8 fa 10 1a cb	3f 1a 1c cb eb b8 c7 3b e9 94 46 91 8e 3f af f3 ae d2 47 a3	

TELIA CERTIFICATION AUTHORITY

CA #	Cert. #	Subject	Issuer	Serial	Key Algorithm and Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA1 Fingerprint	Extended Key Usage
7	1	CN = TeliaSonera Gateway CA v1 O = TeliaSonera	TeliaSonera Root CA v1	35 79 1d 87 92 51 6d 61 b1 1c 4b ef af 76 c1 da	RSA 4096 bits	sha1RSA	13 May 2013	17 October 2032	8f 59 95 28 26 a2 b0 6d 19 49 99 d2 fb b0 84 47 4d cb 95 fc	0d e2 60 f7 96 5c c7 d1 cc be 92 21 26 68 52 9f e5 5f 7d cd	The CA did not issue certificates during the period 1 Apr 2017 to 31 Mar 2018 and was maintained online to provide revocation status information only.
8	1	CN = Telia Domain Validation SSL CA v1 O = Telia Finland Oyj C = FI	TeliaSonera Root CA v1	01 61 ae 20 05 ce 3f 12 7e f8 8d d7 25 1b b1	RSA 4096 bits	sha256RSA	19 February 2018	16 October 2032	49 6c 32 53 7c 5d ed 2b e3 a2 ab 9c 0b c9 5d e4 95 d4 92 5f	8e 16 4d f8 80 51 da 37 8a 68 d8 f4 01 87 6d 29 c1 c7 7c 5b	

The following CAs have not issued publicly trusted SSL/TLS certificates intended to authenticate servers on the Internet (i.e. certificates containing the id-kp-serverAuth OID (1.3.6.1.5.5.7.3.1) in the extendedKeyUsage extension) and they were in scope only for the Network Security Requirements:

CA #	Cert. #	Subject	Issuer	Serial	Key Algorithm and Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA1 Fingerprint	Extended Key Usage
9	1	CN = Telia Document Signing CA v1 O = Telia Finland Oyj C = FI	TeliaSonera Root CA v1	01 60 4b 22 f6 76 3f 09 01 ee 04 83 6b 97 3c	RSA 4096 bits	sha256RSA	28 November 2017	18 October 2032	ee 2a a3 20 42 d6 99 4e 4e 3d 1e 9e 4f e0 b8 a9 9d 74 db fa	59 51 61 ab 72 81 54 58 76 bf 38 ad 93 6c c0 3a b1 2b 8f 90	
10	1	CN = TeliaSonera Class 1 CA v2 O = TeliaSonera C = FI	TeliaSonera Root CA v1	00 fd 41 dd 7f d1 9f 3e e9 f8 5d 9e 43 71 33 d4 db	RSA 4096 bits	sha256RSA	16 October 2014	16 October 2032	d1 47 22 8f cb a8 5d 1a fe 26 41 46 6e cb 82 4b 65 7d 8a e4	89 e3 c8 68 96 af 10 e2 f4 ee cb c8 12 04 6e b9 a4 4c 8f d0	
11	1	CN = TeliaSonera Class 1 CA v1 O = TeliaSonera	TeliaSonera Root CA v1	00 f8 5d 2f 19 0c 60 9f 14 94 b2 8d f9 c1 d1 e7 4c	RSA 4096 bits	sha1RSA	13 May 2013	17 October 2032	f5 ea 33 8c f8 a5 2e 8c a6 82 6b 4d 8b 32 2a a7 b7 53 cf cc	6c 0d 9c 40 94 9c 7e a5 72 a5 b9 48 01 98 8a 9f 19 b4 07 e9	The CA did not issue certificates during the period 1 Apr 2017 to 31 Mar 2018 and was maintained online to provide revocation status information only.
12	1	CN = TeliaSonera Class 2 CA v2 O = TeliaSonera C = SE	TeliaSonera Root CA v1	63 7c 0b d7 85 a5 bf 29 da 60 2d 7c 4d 7a 70 b1	RSA 4096 bits	sha256RSA	16 October 2014	16 October 2032	9e 19 ff e5 0d 3a fe 00 97 15 3f 69 f1 dc 5a 3c aa 0c 94 83	25 5a d6 e3 86 59 63 cf 5a d9 7b 31 2a 26 86 e2 4e db 92 24	

TELIA CERTIFICATION AUTHORITY

CA #	Cert. #	Subject	Issuer	Serial	Key Algorithm and Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA1 Fingerprint	Extended Key Usage
13	1	CN = TeliaSonera Class 2 CA v1 O = TeliaSonera	TeliaSonera Root CA v1	00 d0 d7 72 72 9a 04 17 97 f8 9e da e3 82 f9 1f 11	RSA 4096 bits	sha1RSA	13 May 2013	17 October 2032	d4 6d bd b2 55 bb 52 4b 2a e8 b3 df 6d a7 d8 01 fb 67 9f 72	51 e6 35 0e 44 5c 1f 7c ca a2 7d 5b 6b a2 1d 28 65 ae 04 a4	
14	1	CN = TeliaSonera Email CA v4 O = TeliaSonera C = SE	TeliaSonera Root CA v1	52 eb a0 d8 b7 4b 46 eb 85 57 cd 6d a2 a3 dd dd	RSA 4096 bits	sha256RSA	16 October 2014	16 October 2032	89 86 2a 82 d1 78 fa f0 a6 29 54 35 87 95 6f d3 77 60 19 f0	df fd 4e 47 cf f7 c0 17 0a 53 eb ea 18 20 fb 4f 95 04 60 f5	
15	1	CN = TeliaSonera Email CA v3 O = TeliaSonera	TeliaSonera Root CA v1	00 81 51 ad 72 8b 67 a5 7f a4 55 24 8d 81 d3 57 f9	RSA 4096 bits	sha1RSA	13 May 2013	17 October 2032	f3 74 b8 1d 13 33 d1 c9 ad 5b ce 66 28 9a 99 32 81 f0 20 ce	11 ef 59 16 40 5e 41 0d 0e c7 45 36 f9 f1 90 f6 ed 62 96 29	The CA did not issue certificates during the period 1 Apr 2017 to 31 Mar 2018 and was maintained online to provide revocation status information only.
16	1	CN = Ericsson NL Individual CA v3 O = Ericsson C = SE	TeliaSonera Root CA v1	53 b8 7e 83 e1 9c 99 28 93 b0 9b 49 1c ec b8 eb	RSA 4096 bits	sha256RSA	27 October 2015	27 October 2025	1c 7b 19 9e 97 9c 76 ac 20 3d d8 dc e3 91 6a e3 db 2d a6 53	f5 d9 4b dd 46 fe 6f 7b 3b 29 d0 b0 a4 37 fd 47 96 65 4d e5	The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-emailProtection
17	1	CN = Ericsson NL Individual CA v2 O = Ericsson	TeliaSonera Root CA v1	00 a0 0c cb cc 9b 99 98 ec e2 3a 70 f4 7c c1 c0 59	RSA 4096 bits	sha1RSA	27 May 2014	27 May 2024	b1 0d ca d4 46 b7 af 86 02 c3 2f 6f 06 ca 0e 76 71 7f 4b 37	27 45 1f a5 c9 1d aa bf e4 2e b1 e5 49 07 df 32 a5 b1 58 b0	The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-emailProtection

TELIA CERTIFICATION AUTHORITY

The following CAs in the CA hierarchy were not in the scope of the engagement. These CAs have not issued publicly distributed and trusted subscriber certificates, instead the certificates are only relied by Telia's authentication service.

CA #	Cert. #	Subject	Issuer	Serial	Key Algorithm and Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA1 Fingerprint	Other information
1	1	CN = TeliaSonera Mobile ID CA v2 O = TeliaSonera Finland Oyj C = FI	TeliaSonera Root CA v1	01 61 ae 3e 89 33 e5 b8 95 8a ef 92 9c 0c eb	RSA 4096 bits	sha256RSA	19 February 2018	17 October 2032	d0 2d d3 14 f0 77 4a 62 27 2c 65 53 93 d5 a5 a5 43 af c2 52	16 6a 7f a3 7f eb 9f 97 87 ea b2 69 88 a0 98 ca 27 ae 04 0b	The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-timeStamping
	2	CN = TeliaSonera Mobile ID CA v2 O = TeliaSonera Finland Oyj C = FI	TeliaSonera Root CA v1	03 75 c4 9b 7e 63 ce 43 37 07 ff 19 84 37 a5 ef	RSA 4096 bits	sha256RSA	26 January 2016	17 October 2032	d0 2d d3 14 f0 77 4a 62 27 2c 65 53 93 d5 a5 a5 43 af c2 52	57 b2 20 23 1d c6 b6 9c a5 0a cc c9 bc 66 b0 84 9b aa 78 2a	The certificate has been revoked 17 Apr 2018. The CA certificate had the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-emailProtection id-kp-timeStamping
2	1	CN = TeliaSonera Mobile ID CA v1 O = TeliaSonera Finland Oyj C = FI	TeliaSonera Root CA v1	01 63 8b ea 73 4a fa f8 7f 6e 51 24 37 1f 72	RSA 4096 bits	sha256RSA	23 May 2018	16 October 2032	53 80 2c e5 18 4b 1e c1 0b d6 26 2c d1 08 ef 88 86 dd 2c 0e	68 a5 35 9c a1 c7 72 33 ca 27 66 3f 1d 29 7e e8 43 62 a1 22	The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth
	2	CN = TeliaSonera Mobile ID CA v1 O = Telia Finland Oyj C = FI	TeliaSonera Root CA v1	01 62 af 14 90 9a 4c 15 5a 56 ba 6d b7 ab 5f	RSA 4096 bits	sha256RSA	10 April 2018	16 October 2032	53 80 2c e5 18 4b 1e c1 0b d6 26 2c d1 08 ef 88 86 dd 2c 0e	90 ef e8 0c da 70 af 07 10 93 8f c6 a9 d0 60 9c 0c f4 4a ba	The certificate has been revoked 23 May 2018. The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth

TELIA CERTIFICATION AUTHORITY

CA #	Cert. #	Subject	Issuer	Serial	Key Algorithm and Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA1 Fingerprint	Other information
	2	CN = TeliaSonera Mobile ID CA v1 O = TeliaSonera Finland Oyj C = FI	TeliaSonera Root CA v1	00 d7 6a 8b c5 05 09 00 a1 9b 44 5c 87 28 cc a6 36	RSA 4096 bits	sha256RSA	16 October 2014	16 October 2032	53 80 2c e5 18 4b 1e c1 0b d6 26 2c d1 08 ef 88 86 dd 2c 0e	80 2f f3 0f b8 b6 26 63 35 c2 fc a8 6e 20 c3 df ff fd 6a 19	The certificate has been revoked 17 Apr 2018. The CA certificate had the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-emailProtection
	3	CN = TeliaSonera Mobile ID CA v1 O = TeliaSonera Finland Oyj C = FI	TeliaSonera Root CA v1	00 f9 4c 94 77 c4 fb 88 be 33 5e 65 72 d3 7a 72 25	RSA 4096 bits	sha256RSA	16 December 2010	17 October 2032	53 80 2c e5 18 4b 1e c1 0b d6 26 2c d1 08 ef 88 86 dd 2c 0e	cb 18 ac 54 e8 d1 6c 01 93 dd 95 4e 18 53 7b 8a 71 b2 34 e7	