TELIA'S MANAGEMENT’S ASSERTION

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

The management of Telia has assessed its disclosure 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:

<table>
<thead>
<tr>
<th>#</th>
<th>Observation</th>
<th>Relevant WebTrust Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>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.</td>
<td>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</td>
</tr>
</tbody>
</table>

Based on that assessment, in Telia management's opinion, except for the matters as 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 2019 to 31 March 2020, Telia has:

- disclosed its SSL certificate life cycle management business practises in its:
  - Telia Production Certification Practice Statement, version 2.8, dated March 2020

- 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 lifecycles; 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 v2.4.

Helsinki, 26 June 2020
Telia Company AB

[Signature]

Tommi Mattila
Head of Product Area, IT Services
## Attachment A: List of CAs in scope

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

<table>
<thead>
<tr>
<th>No.</th>
<th>CA Subject</th>
<th>Issuer</th>
<th>Serial</th>
<th>Key Algorithm</th>
<th>Key Size</th>
<th>Digest Algorithm</th>
<th>Not Before</th>
<th>Not After</th>
<th>SKI</th>
<th>SHA2 Fingerprint</th>
<th>Other Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CN = TeliaSonera Root CA v1 O = TeliaSonera</td>
<td>Self-signed</td>
<td>0095BE16A 0F72E46F1 7698B272F A8BCD96</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha1RSA</td>
<td>18 October 2007</td>
<td>18 October 2092</td>
<td>F08F593800B 3F5F9A960C D5EBA79A A17E81312</td>
<td>DD6596E1F21F8F077 C123A1A21C12224F 7255B73E03A72806 93E8A420FA389</td>
<td>Cross-certificate</td>
</tr>
<tr>
<td>2</td>
<td>CN = TeliaSonera Root CA v1 O = TeliaSonera</td>
<td>Sonera Class2 CA</td>
<td>876D2E1A2 82F4AC519 AA3AEB8B0 DA2CB</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>5 December 2014</td>
<td>5 April 2021</td>
<td>F08F593800B 3F5F9A960C D5EBA79A A17E81312</td>
<td>E96F6581E712CB290F 23A749346535E0B0D 81E3D4A3D56D0D64 884C0B81688CB9</td>
<td>Cross-certificate</td>
</tr>
<tr>
<td>3</td>
<td>CN = Telia Root CA v2 O = Telia Finland Oyj C = FI</td>
<td>Self-signed</td>
<td>01675F27D 6E7A3E3E4 ACBE095B0 56E</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018</td>
<td>29 November 2043</td>
<td>72ACE43379A A45876F6DA C1D86D6C72 F86D82439</td>
<td>242B69742FC1B16B2 ABF988998D9472167 544E540D91178657 3621F6A74B82C</td>
<td>Cross-certificate</td>
</tr>
<tr>
<td>4</td>
<td>CN = TeliaSonera Root CA v1 O = TeliaSonera</td>
<td>TeliaSonera Root CA v1</td>
<td>01875F82B E0017DE89 55A9376EB 1F9</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018</td>
<td>29 November 2032</td>
<td>72ACE43379A A45876F6DA C1D86D6C72 F86D82439</td>
<td>E6F62963F6D6B12D 7G5312F4F13419E 7C2877678B3E4A9087 AD5869468467F</td>
<td>Cross-certification</td>
</tr>
<tr>
<td>5</td>
<td>CN = TeliaSonera Server CA v2 O = TeliaSonera</td>
<td>TeliaSonera Root CA v1</td>
<td>4C462AF6D BFBF7804F 84C17C6EA 972B6</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>2F603C294FD 7072F9C8B8 D56F5663D1 2832295</td>
<td>D711110388CA8F20B BA9F1A8D8A4EF8B C16392A3DEBA697C 53E6A0ACACAC</td>
<td>Cross-certification</td>
</tr>
<tr>
<td>CA #</td>
<td>Cert #</td>
<td>Subject</td>
<td>Issuer</td>
<td>Serial</td>
<td>Key Algorithm</td>
<td>Key Size</td>
<td>Digest Algorithm</td>
<td>Not Before</td>
<td>Not After</td>
<td>SKI</td>
<td>SHA2 Fingerprint</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>---------</td>
<td>--------</td>
<td>--------</td>
<td>---------------</td>
<td>----------</td>
<td>------------------</td>
<td>------------</td>
<td>-----------</td>
<td>-----</td>
<td>-----------------</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>CN = TeliaSonera Gateway CA v2 O = TeliaSonera C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>00863C7564 1105854FB4 3138A0A0C F6AA3</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>87AAE313129 F118BCA68C D1E2DC429A 6FA101ACB</td>
<td>462BD88788E02CA8F 5D85D67ED8C84B19 45B3820568B160421 99D540CA9E298</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>CN = Telia Extended Validation CA v3 O = Telia Finland Oyj C = FI</td>
<td>Telia Root CA v2</td>
<td>01675FAC7 2694C74BF 1A67EDC1B 3AD</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2016</td>
<td>29 November 2043</td>
<td>FB36703B5D1 FF07DB220B9 C0E92EB7D9 E850A835</td>
<td>98C2545A2C0A5A342E DB22A9F6C7CC1F E98DE759567E3A29 8AD9F70B1291D</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>CN = Telia Domain Validation SSL CA v1 O = Telia Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>0161AE200 5C3E8127E F880D7251 B81</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>19 February 2018</td>
<td>16 October 2032</td>
<td>496C32537C5 DED2BE3A2A B9C0BC95DE 4950492F</td>
<td>2154A96A1496590C F29A887E2A470B49 8A1799786A264</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>CN = Telia Domain Validation CA v3 O = Telia Finland Oyj C = FI</td>
<td>Telia Root CA v2</td>
<td>01675FFDE 7E41811E2 C07800CD B50A</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2016</td>
<td>29 November 2043</td>
<td>5BF1EE298D 31B23B3AE01 7CBA407E53 F8242FA3</td>
<td>A7E83056E9B3D09DD B161DB95DF196A5E5 A1DFDF28F603B 1C58556EAA463</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>CN = Telia Domain Validation CA v2 O = Telia Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>016854E34 A3BDE9E63 E86ED2174 764</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 August 2018</td>
<td>18 October 2032</td>
<td>ED3D749C2C 53B871937B4 B11F6B891E2 82F962DB</td>
<td>5B312B7E11B70D07 C140AB99F080D07 48966096C652A85A0 6A6822BEB59A02C</td>
</tr>
<tr>
<td>CA #</td>
<td>Cert #</td>
<td>Subject</td>
<td>Issuer</td>
<td>Serial</td>
<td>Key Algorithm</td>
<td>Key Size</td>
<td>Digest Algorithm</td>
<td>Not Before</td>
<td>Not After</td>
<td>SKI</td>
<td>SHA2 Fingerprint</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>---------</td>
<td>--------</td>
<td>--------</td>
<td>---------------</td>
<td>----------</td>
<td>------------------</td>
<td>------------</td>
<td>-----------</td>
<td>-----------</td>
<td>------------------------</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>CN = Telia Server CA v3</td>
<td>Telia Root CA v2</td>
<td>01675FE78 F10F349257 F19B3731F</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018</td>
<td>29 November 2043</td>
<td>4666BD0E072 1281AD8FA8EB83F2</td>
<td>31680E4F05 730A7688CB813A270</td>
</tr>
<tr>
<td></td>
<td></td>
<td>O = Telia Finland Oyj C = FI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To the Management of Telia Company AB (Telia)

Amstelveen, 26 June 2020

Subject: Independent Auditor’s Report WebTrust for CAs Baseline Requirements

We have been engaged, in a reasonable assurance engagement, to report on Telia’s management’s assertion that for its Certification Authority (CA) operations in Finland and Sweden, throughout the period 1 April 2019 through 31 March 2020 for its CAs as enumerated in Attachment A, Telia has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - Telia Production Certification Practice Statement, version 2.8, March 2020

including its commitment to provide SSL Certificates in conformity with the CA/Browser Forum Guidelines, as published 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 lifecycles; 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 v2.4.

Certification Authority’s responsibilities

Telia’s management is responsible for its assertion, 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 v2.4.

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. Therefore, we are independent of Telia and complied with other ethical requirements in accordance with the Code of Ethics of NOREA and the Code of Ethics for Professional Accountants (a regulation with respect to independence) of the NBA, Royal Netherlands Institute of Chartered Accountants.

We apply the International Standard on Quality Control 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. We also apply the Regulations for Quality management systems of the NBA and, accordingly, maintain 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 assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements (ISAE) 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board and the related Dutch Directive 3000A ‘Attestation engagements’, as issued by NOREA, the IT Auditors Association in The Netherlands.

These standards requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management’s assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding of Telia’s SSL certificate lifecycle 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 key and certificate lifecycle management business 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’ 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.
Subject: Independent Auditor Report WebTrust for CAs Baseline Requirements
Amstelveen, 26 June 2020

Basis for qualified opinion

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

<table>
<thead>
<tr>
<th>Observation</th>
<th>Relevant WebTrust Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>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</td>
</tr>
</tbody>
</table>

Qualified opinion

In our opinion, except for the matters described in the basis for qualified opinion section above, throughout the period 1 April 2019 through 31 March 2020, Telia has, in all material respects:

- disclosed its SSL certificate life cycle management business practices in its:
  - Telia Production Certification Practice Statement, version 2.8, March 2020
  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 lifecycles; 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 v2.4.

This report does not include any representation as to the quality of Telia’ services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4, nor the suitability of any of Telia’ services for any customer’s intended purpose.

**Use of the WebTrust seal**

Telia’ use of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

On behalf of KPMG Advisory N.V.
Amstelveen, 26 June 2020

(originally signed by)

drs. ing. R.F. Koorn RE CISA
Partner
Attachment A: List of CAs in scope
The following CAs were in scope of the engagement:

<table>
<thead>
<tr>
<th>CA #</th>
<th>Cert #</th>
<th>Subject</th>
<th>Issuer</th>
<th>Serial</th>
<th>Key Algorithm</th>
<th>Key Size</th>
<th>Digest Algorithm</th>
<th>Not Before</th>
<th>Not After</th>
<th>SKI</th>
<th>SHA2 Fingerprint</th>
<th>Other information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>CN = TeliaSonera Root CA v1</td>
<td>Self-signed</td>
<td>0095BE16A0F7 2E46F17B39827 2FA8BACD96</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha1RSA</td>
<td>18 October 2007</td>
<td>18 October 2032</td>
<td>F08F593800B3F5 8F9A960CD5EBF A7BAA17E81312</td>
<td>DD6936FE21F8F077 C123A1A521C12224F 72255B73E03A72606 93E8A2B0FA389</td>
<td>Cross-certificate</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>CN = TeliaSonera Root CA v1</td>
<td>Self-signed</td>
<td>87ED2E1A2B286 4AC519AA33EA B90DA2CB</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>5 December 2014</td>
<td>5 April 2021</td>
<td>F08F593800B3F5 8F9A960CD5EBF A7BAA17E81312</td>
<td>E956358F17E12B890 23A474934653EBD9 81E3D4A39D56D604 684CD0B1698C89</td>
<td>Cross-certificate</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>CN = TeliaSonera Root CA v2</td>
<td>Self-signed</td>
<td>01675F27D6FE 7AE3E4ACBE09 5B059E</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018</td>
<td>29 November 2043</td>
<td>72ACE43379A4 587F6FDAC1D9E D6C72F6B62439</td>
<td>242B69742FCB1E5B2 ABF9898BB94572187 544E5B4D991176857 3621F6A7482C</td>
<td>Cross-certificate</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>CN = TeliaSonera Root CA v2</td>
<td>Self-signed</td>
<td>01675F82E001 7DE8955FA937 6B1E9F</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018</td>
<td>10 March 2032</td>
<td>72ACE43379A4 587F6FDAC1D9E D6C72F6B62439</td>
<td>E6F929F36F62BD 4753122F41F341EE 7C2877578BEA9807 ADF5B94658E7F</td>
<td>Cross-certificate</td>
</tr>
<tr>
<td>CA #</td>
<td>Cert #</td>
<td>Subject</td>
<td>Issuer</td>
<td>Serial</td>
<td>Key Algorithm</td>
<td>Key Size</td>
<td>Digest Algorithm</td>
<td>Not Before</td>
<td>Not After</td>
<td>SKI</td>
<td>SHA2 Fingerprint</td>
<td>Other Information</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>---------</td>
<td>--------</td>
<td>--------</td>
<td>---------------</td>
<td>----------</td>
<td>-----------------</td>
<td>--------------</td>
<td>--------------</td>
<td>-----</td>
<td>-----------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>CN = TeliaSonera Gateway CA v2 O = TeliaSonera C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>00863C7564119 5854FBA43136A0 A00F8AA3</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>87AAE313129F11</td>
<td>8BCA68CD1E2DC</td>
<td>429A8FA101ACB</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>CN = Telia Extended Validation CA v3 O = Telia Finland Oyj C = FI</td>
<td>Telia Root CA v2</td>
<td>01675FAC7299 4C74BF1A67ED C1B3AD</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018</td>
<td>29 November 2043</td>
<td>FB36703B5D1FF0</td>
<td>7DB22089CE0E2</td>
<td>EB7D9E85A835</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>CN = Telia Domain Validation SSL CA v1 O = Telia Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>0161AE2005CE 3F127EF88DD7 251BB1</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>19 February 2018</td>
<td>16 October 2032</td>
<td>496C325375C5DF</td>
<td>D2BE3A2AB9C0B</td>
<td>C95DE495D4925</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>CN = Telia Domain Validation CA v3 O = Telia Finland Oyj C = FI</td>
<td>Telia Root CA v2</td>
<td>01675FFEDE7E4 1811E2CD76B0 CD550A</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018</td>
<td>29 November 2043</td>
<td>5BF1E2E92D31B</td>
<td>23B3AE017CBA4</td>
<td>07EF9B2421F3A</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>CN = Telia Domain Validation CA v2 O = Telia Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>016584E34A38 D9963E3BEED 2174784</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 August 2018</td>
<td>18 October 2032</td>
<td>ED3D749C2C53B</td>
<td>B719375B11F6B</td>
<td>891E282F992DB</td>
</tr>
</tbody>
</table>
## Subject: Independent Auditor Report WebTrust for CAs Baseline Requirements

Amstelveen, 26 June 2020

<table>
<thead>
<tr>
<th>CA #</th>
<th>Cert #</th>
<th>Subject</th>
<th>Issuer</th>
<th>Serial</th>
<th>Key Algorithm</th>
<th>Key Size</th>
<th>Digest Algorithm</th>
<th>Not Before</th>
<th>Not After</th>
<th>SKI</th>
<th>SHA2 Fingerprint</th>
<th>Other Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>1</td>
<td>CN = Telia Server CA v3</td>
<td>Telia Root CA v2</td>
<td>0167FE78F10F 349257F16B373 1F7A</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018</td>
<td>29 November 2043</td>
<td>46668D0E072316 B0EA4F05EB965 ADEA5EEC97EA4</td>
<td>FAD48F5F5E589A</td>
<td></td>
</tr>
</tbody>
</table>