To the Management of Telia Company AB

Amstelveen, 27 June 2022

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

We have been engaged, in a reasonable assurance engagement, to report on Telia Company AB’s (Telia) management’s assertion that for its Certification Authority (CA) operations in Finland and Sweden, throughout the period 1 April 2021 through 31 March 2022 for its CAs as enumerated in Attachment A, Telia has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - *Certificate Policy and Certification Practice Statement for Telia Client Certificates, version 3.2*, dated October 2021
  - *Certificate Policy and Certification Practice Statement for Telia Server Certificates, version 4.4*, dated October 2021

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 v2.5.

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 v2.5.

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 (IT Auditors Association in The Netherlands) 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 ‘Reglement Kwaliteitsbeheersing NOREA’ (RKBN, Regulations for Quality management systems) 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.

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
Subject: Independent Auditor Report WebTrust for CAs Baseline Requirements
Amstelveen, 27 June 2022

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 assess-
ments 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 aforementio-
ned 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:

<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 2021 through 31 March 2022, Telia has, in all material respects:

- disclosed its SSL certificate life cycle management business practices in its:
  - Certificate Policy and Certification Practice Statement for Telia Server Certificates, version 4.4, dated October 2021

  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;
Subject: Independent Auditor Report WebTrust for CAs Baseline Requirements
Amstelveen, 27 June 2022

- 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 v2.5.

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 v2.5, nor the suitability of any of Telia’ services for any customer’s intended purpose.

Use of the WebTrust seal

Telia’s 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, 27 June 2022

Original 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 WebTrust for CAs Baseline Requirements Audit:

<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>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 O = TeliaSonera</td>
<td>Self-signed</td>
<td>0095BE16A0F 72E46F17B398 272FA8BCD96</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha1RSA</td>
<td>18 October 2007 18 October 2032</td>
<td>F08F593800B3F58 F9A960CD5EBFAF7 BAA17E81312</td>
<td>DD6936FE21F6F077C123A1A 521C12224F72255B73E03A72 60693E8A24B0FA389</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>CN = TeliaSonera Root CA v1 O = TeliaSonera</td>
<td>Sonera Class2 CA</td>
<td>87ED2E1A282 64AC519AA3A EBB90DA2CB</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>5 December 2014 5 April 2021</td>
<td>F08F593800B3F58 F9A960CD5EBFAF7 BAA17E81312</td>
<td>E9563581E712B290F23A7493 46535EB0D981E3D4A39D56D 604684CD081698C89</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>CN = Sonera Class2 CA O = Sonera C = FI</td>
<td>Self-signed</td>
<td>1D</td>
<td>RSA</td>
<td>2048 bits</td>
<td>sha1RSA</td>
<td>16 April 2001 16 April 2021</td>
<td>4AA0AA5884D35E</td>
<td>3C</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>CN = Telia Root CA v2 O = Telia Finland Oyj C = FI</td>
<td>Self-signed</td>
<td>01675F27D6F E7AE3E4ACB E095B059E</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018 29 November 2043</td>
<td>72ACE43379AA45 87F6FDAC19D8ED672F86D82439</td>
<td>242B69742FCB1E5B2ABF988 98B94572187544E584D99117 86573621F6A74B82C</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>CN = Telia Root CA v2 O = Telia Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>01675F62BE00 17DE8955A93 76E81F9</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018 18 October 2032</td>
<td>72ACE43379AA45 87F6FDAC19D8ED672F86D82439</td>
<td>EF6F29F636F628DD4753122F 41F3419EE7C2877587BE4A98 07ADF5894658E7F</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>CN = TeliaSonera Server CA v2 O = TeliaSonera C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>4C462AF6DBF BF7804F84C1 7CFEA972B6</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014 16 October 2032</td>
<td>2F493C294FD7072 5F9C58CD546F56 63D12832295</td>
<td>D721110388CA6F20BA9FD1 A80BA4EBC6139243DEBA D97C553EEAF0ACACA</td>
</tr>
</tbody>
</table>
## Subject: Independent Auditor Report WebTrust for CAs Baseline Requirements
### Amstelveen, 27 June 2022

<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>5</td>
<td>1</td>
<td>CN = TeliaSonera Gateway CA v1</td>
<td>TeliaSonera Root CA v1</td>
<td>00863C75641195854FB43138A0A0CF8AA3</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>87AAE313129F118BCA68CD1E2DC429A8FA101ACB</td>
<td>46226B7B80E02CA8F3D85D67ED8CB4B19C48382059BB16242195D540CABE9289</td>
<td>Revoked (Cessation Of Operation) 28 April 2021</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>CN = Telia Domain Validation CA v3</td>
<td>Telia Root CA v2</td>
<td>01675FFDE7E41811E2CD70B0CDB50A</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018</td>
<td>29 November 2043</td>
<td>5BF1EE298D31B23B3AE017BCBA407E93F82421FA3</td>
<td>A7E53056E983D9DB1816B95518F6A5E5A1DFDFA26F60533B1C850855EA4263</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>CN = Telia Domain Validation CA v3</td>
<td>TeliaSonera Root CA v1</td>
<td>016584E34A38D98963E8EBED217478A</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 August 2018</td>
<td>18 October 2032</td>
<td>E0D3D749C2C53B71937B4116B891E282F992DB</td>
<td>5B312B7E111B7D07C14E0AB99F080074896806C52AA85A06ABA22B8E5A02C</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>CN = Telia Server CA v3</td>
<td>Telia Root CA v2</td>
<td>01675FE78F10F349257F16B3731F7A</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018</td>
<td>29 November 2043</td>
<td>46668DDE0E7231B0E4A0F0E3965AD9A5EEC97EA4</td>
<td>1281AD8FABE883F209E9636448DA180C373DA7686C813A270FAD48F5E698A</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>CN = TeliaSonera Class 1 CA v2</td>
<td>TeliaSonera Root CA v1</td>
<td>00FD41DD7FD19F3EEF86B59E43713D34D</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>D147228FCBA85D1AFE264166EC824B657D8AE4</td>
<td>B95AE54F838E3ABF0B57ACC1B1266DC68C7A3F7A47015FA128D60CD1AAE280</td>
<td></td>
</tr>
</tbody>
</table>
Subject: Independent Auditor Report WebTrust for CAs Baseline Requirements  
Amstelveen, 27 June 2022

<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>
</table>
| 10   | 1      | CN = TeliaSonera Class 2 CA v2  
O = TeliaSonera  
C = SE | TeliaSonera Root CA v1 | 637C0BD785A  
5BF29DA602D  
7C4D7A7DB1 | RSA | 4096 bits | sha256RSA | 16 October 2014 | 16 October 2032 | 9E19FFE50D3AFE  
0097153F69F1DC5  
A3CAA0C94B3 | 092829433D231949F4A9BC6  
6CBF54B3AA27D7B3ECA048  
D75E59093E15A72EA5 |                      |
| 11   | 1      | CN = TeliaSonera Email CA v4  
O = TeliaSonera  
C = SE | TeliaSonera Root CA v1 | 52EBA0D8874  
B46E8557CD  
6DA2A3DDDA | RSA | 4096 bits | sha256RSA | 16 October 2014 | 16 October 2032 | 89862A82D178FAF  
0A629543587956F  
D776019F0 | D1F2656AC8382739A3B087C  
47AB5CAB945A32F1026149  
C308783C7E06AF8AE8 |                      |
Attachment B: Publicly disclosed incidents

<table>
<thead>
<tr>
<th>#</th>
<th>Disclosure</th>
<th>Publicly Disclosed Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Invalid email contact address was used for few domains</td>
<td><a href="#">Bugzilla Ticket Link</a></td>
</tr>
<tr>
<td>2</td>
<td>Delayed revocation of 5 EE certificates in connection to id=1736020</td>
<td><a href="#">Bugzilla Ticket Link</a></td>
</tr>
<tr>
<td>3</td>
<td>Issued three pre-certificates with non-NIST EC curve</td>
<td><a href="#">Bugzilla Ticket Link</a></td>
</tr>
</tbody>
</table>
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 deviation 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 2021 to 31 March 2022, Telia has:

- disclosed its SSL certificate life cycle management business practices in its:
  - Certificate Policy and Certification Practice Statement for Telia Server Certificates, version 4.4, dated October 2021
  - 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:
  o logical and physical access to CA systems and data is restricted to authorized individuals;
  o the continuity of key and certificate management operations is maintained; and
  o 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 v2.5.

Helsinki, 27 June 2022

Telia Company AB

Original signed by

Tomi Hautala

Head of Trust 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>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 O = TeliaSonera</td>
<td>Self-signed</td>
<td>0095BE16A0F 72E46F17B398 272FA8BCD96</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha1RSA</td>
<td>18 October 2007</td>
<td>18 October 2032</td>
<td>F08F593800B3F58 F9A960CD5EBFA7 BAA17E81312</td>
<td>DD6936FE21F8F077C 123A1A521C1222F72 255B73E03A7260693E 8A24B0FA389</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>CN = TeliaSonera Root CA v1 O = TeliaSonera</td>
<td>Sonera Class2 CA</td>
<td>87ED2E1A282 64AC519AA3A EBB90DA2CB</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>5 December 2014</td>
<td>5 April 2021</td>
<td>F08F593800B3F58 F9A960CD5EBFA7 BAA17E81312</td>
<td>E9563581E712B290F 3A74934655EBD981 E3D4A39D56D60468 CD0B1698C89</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>CN = Sonera Class2 CA O = Sonera C = FI</td>
<td>Self-signed</td>
<td>1D</td>
<td>RSA</td>
<td>2048 bits</td>
<td>sha1RSA</td>
<td>16 April 2001</td>
<td>16 April 2021</td>
<td>4AA0AA5884D3E3C</td>
<td>Expired 16 April 2021</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>CN = Telia Root CA v2 O = Telia Finland Oyj C = FI</td>
<td>Self-signed</td>
<td>01675F27D6F E7AE3E4AC8 E095B059E</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018</td>
<td>29 November 2043</td>
<td>72ACE43379AA445 87F6F6DAC1D9ED6 C72F86D82439</td>
<td>242B69742FCB15E5B 4A5F9898B945721875 44E5B4D9117865736 21F6A74B82C</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>CN = Telia Root CA v2 O = Telia Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>01675F82BE00 17DE8955A93 76EB1F9</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018</td>
<td>18 October 2032</td>
<td>72ACE43379AA445 87F6F6DAC1D9ED6 C72F86D82439</td>
<td>242B69742FCB15E5B 4A5F9898B945721875 44E5B4D9117865736 21F6A74B82C</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>CN = TeliaSonera Server CA v2 O = TeliaSonera C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>4C462AF6DBF BF7804F84C1 7CFEA972B6</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>2F493C294FD7072 5F9C68CD64F56 63D12832295</td>
<td>D721110388CA6F20B BA9FD1ADBAA4EFF8 C16392A3DEBAD97C5 53EEA0ACAAAC</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>00863C756411 95854FB43138 B0CDB95A</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>87AAE313129F11F BCA68CD64F2D4 C9A8FA101ACB</td>
<td>46226B7B89E02CA8F 5D85D60D86C48B19C 48382058BB16242199 D540CABE9268</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>CN = Telia Domain Validation CA v3</td>
<td>Telia Root CA v2</td>
<td>01675FDE7E 41811E2CD76 B0CDB95A</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018</td>
<td>29 November 2043</td>
<td>5BF1EE29B83D1B 3B3AE0117CBA407 E93F82421FA3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Expired 16 April 2021
Revoked (Cessation Of Operation) 28 April 2021
Cross-certificate, Expired 5 April 2021
<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>7</td>
<td>1</td>
<td>CN = Telia Domain Validation Root CA v1</td>
<td>TeliaSonera</td>
<td>016584E34A38</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 August 2018</td>
<td>18 October 2032</td>
<td>ED3D749C2C53BB71937B4B11F6B891E282F992DB</td>
<td>5B31287E11B70D07C14E0AB99F080D0074896608C52AAB5A06A0822BBE592A0E2</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>CN = Telia Server CA v3</td>
<td>Telia Root CA v2</td>
<td>01675FE78F10F349257F16B3731F7A</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>29 November 2018</td>
<td>29 November 2043</td>
<td>46668DD0E072316D0EA4F05EB965ADEA5EEC97EA4</td>
<td>1281AD8FABE883F209E9636448D1A80C373DAA7886C813A270FA43F5F5E592A</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>CN = TeliaSonera Class 1 CA v2</td>
<td>TeliaSonera Root CA v1</td>
<td>00FD41DD7FD19F3E9F85D9E437133D4D</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>D147228FCBA85D1AFE2641466ECB824B657DAE4</td>
<td>B95AE54F83B3ABFO57ACC1B1266DC68C7A3FA774015FA12848DD1AEE280</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>CN = TeliaSonera Class 2 CA v2</td>
<td>TeliaSonera Root CA v1</td>
<td>637C8BD785A5BF29DA602D7C4D7A70B1</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>9E19FE50D3A9E27F69F1DC5A3CAA0C9483109282943DD231949F4A9BC666CBF54B3AA27D7BEBCA04075E59093E1572A5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>CN = TeliaSonera Email CA v4</td>
<td>TeliaSonera Root CA v1</td>
<td>52EBA0D8B74B4E68B557CD6DA2A3DDBD</td>
<td>RSA</td>
<td>4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>89862A82D178FA0A629543587956FDD776019F0</td>
<td>D1F2655AC83B27393A3B07C747A5CB945A32F162B61493C808783C7E06AF8AE8</td>
<td></td>
</tr>
</tbody>
</table>
# Attachment B: Publicly disclosed incidents

<table>
<thead>
<tr>
<th>#</th>
<th>Disclosure</th>
<th>Publicly Disclosed Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Invalid email contact address was used for few domains</td>
<td>Bugzilla Ticket Link</td>
</tr>
<tr>
<td>2</td>
<td>Delayed revocation of 5 EE certificates in connection to id=1736020</td>
<td>Bugzilla Ticket Link</td>
</tr>
<tr>
<td>3</td>
<td>Issued three precertificates with non-NIST EC curve</td>
<td>Bugzilla Ticket Link</td>
</tr>
</tbody>
</table>