



**KPMG Advisory N.V.**  
P.O. Box 74500  
1070 DB Amsterdam  
The Netherlands

Laan van Langerhuize 1  
1186 DS Amstelveen  
The Netherlands  
Telephone +31 (0)20 656 7890  
www.kpmg.com/nl

## **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.



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

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' 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' 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 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, 27 June 2022

## Basis for qualified opinion

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

| Observation  | Relevant WebTrust Criteria   |
|--|--|
| <p>1 The Key Usage extension in the root CA certificates of <i>TeliaSonera Root CA v1</i> and <i>Sonera Class 2 CA</i> is not marked critical and <i>TeliaSonera Root CA v1</i> 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.</p> <p>However, Telia generated a new root CA, <i>Telia Root CA v2</i>, on 29 November 2018, which is planned to eventually replace <i>TeliaSonera Root CA v1</i> and <i>Sonera Class 2 CA</i>. Extensions, key sizes, and Certificate Policy Identifiers (including Reserved Certificate Policy Identifiers) of the new <i>Telia Root CA v2</i> certificate conform to the Baseline Requirements.</p> | <p><b>Principle 2, Criteria 2.3</b></p> <p>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</p> |

## 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:
  - o [Certificate Policy and Certification Practice Statement for Telia Client Certificates, version 3.2](#), dated October 2021
  - o [Certificate Policy and Certification Practice Statement for Telia Server Certificates, version 4.4](#), dated October 2021including 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:
  - o the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - o 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;



*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



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

### Attachment A: List of CAs in scope

The following CAs were in scope of the WebTrust for CAs Baseline Requirements Audit:

| CA # | Cert # | Subject   | Issuer                 | Serial                             | Key Algorithm | Key Size  | Digest Algorithm | Not Before       | Not After        | SKI                                      | SHA2 Fingerprint  | Other information                       |
|------|--------|---|------------------------|------------------------------------|---------------|-----------|------------------|------------------|------------------|--|---|---|
| 1    | 1      | CN = TeliaSonera Root CA v1<br>O = TeliaSonera              | Self-signed            | 0095BE16A0F72E46F17B398272FA8BCD96 | RSA           | 4096 bits | sha1RSA          | 18 October 2007  | 18 October 2032  | F08F593800B3F58F9A960CD5EBFA7BAA17E81312 | DD6936FE21F8F077C123A1A521C12224F72255B73E03A7260693E8A24B0FA389  |   |
| 1    | 2      | CN = TeliaSonera Root CA v1<br>O = TeliaSonera              | Sonera Class2 CA       | 87ED2E1A28264AC519AA3AEBB90DA2CB   | RSA           | 4096 bits | sha256RSA        | 5 December 2014  | 5 April 2021     | F08F593800B3F58F9A960CD5EBFA7BAA17E81312 | E9563581E712B290F23A749346535EB0D981E3D4A39D56D604684CD0B1698C89  | Cross-certificate, Expired 5 April 2021 |
| 2    | 1      | CN = Sonera Class2 CA<br>O = Sonera<br>C = FI               | Self-signed            | 1D                                 | RSA           | 2048 bits | sha1RSA          | 16 April 2001    | 16 April 2021    | 4AA0AA5884D35E3C                         | 7908B40314C138100B518D0735807FFBFCF8518A0095337105BA386B153DD927  | Expired 16 April 2021                   |
| 3    | 1      | CN = Telia Root CA v2<br>O = Telia<br>Finland Oyj<br>C = FI | Self-signed            | 01675F27D6FE7AE3E4ACBE095B059E     | RSA           | 4096 bits | sha256RSA        | 29 November 2018 | 29 November 2043 | 72ACE43379AA4587F6FDAC1D9ED6C72F86D82439 | 242B69742FCB1E5B2ABF98898B94572187544E5B4D9911786573621F6A74B82C  |   |
| 3    | 2      | CN = Telia Root CA v2<br>O = Telia<br>Finland Oyj<br>C = FI | TeliaSonera Root CA v1 | 01675F82BE0017DE8955A9376EB1F9     | RSA           | 4096 bits | sha256RSA        | 29 November 2018 | 18 October 2032  | 72ACE43379AA4587F6FDAC1D9ED6C72F86D82439 | EF6F29F636F62BDD4753122F41F3419EE7C2877587BE4A9807ADF58946458E7F  | Cross-certificate                       |
| 4    | 1      | CN = TeliaSonera Server CA v2<br>O = TeliaSonera<br>C = FI  | TeliaSonera Root CA v1 | 4C462AF6DBFBF7804F84C17CFEA972B6   | RSA           | 4096 bits | sha256RSA        | 16 October 2014  | 16 October 2032  | 2F493C294FD70725F9C68CD564F5663D12832295 | D721110388CA6F20BBA9FD1A8DBA4EFB8C16392A3DEBA D97C553EEAF0ACACAAC |   |



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

| CA # | Cert # | Subject   | Issuer                    | Serial   | Key Algorithm | Key Size     | Digest Algorithm | Not Before          | Not After           | SKI  | SHA2 Fingerprint   | Other information                                    |
|------|--------|---|---------------------------|--|---------------|--------------|------------------|---------------------|---------------------|--|--|--|
| 5    | 1      | CN =<br>TeliaSonera<br>Gateway<br>CA v2<br>O =<br>TeliaSonera<br>C = FI           | TeliaSonera<br>Root CA v1 | 00863C756411<br>95854FB43138<br>A0A0CF8AA3     | RSA           | 4096<br>bits | sha256RSA        | 16 October<br>2014  | 16 October<br>2032  | 87AAE313129F118<br>BCA68CD1E2DC4<br>29A8FA101ACB | 46226B7B89E02CA8F5D85D6<br>7ED8CB4B19C48382058BB16<br>242199D540CABE9268 | Revoked (Cessation<br>Of Operation) 28 April<br>2021 |
| 6    | 1      | CN = Telia<br>Domain<br>Validation<br>CA v3<br>O = Telia<br>Finland Oyj<br>C = FI | Telia Root<br>CA v2       | 01675FFDE7E<br>41811E2CD76<br>B0CDB50A         | RSA           | 4096<br>bits | sha256RSA        | 29 November<br>2018 | 29 November<br>2043 | 5BF1EE298D31B2<br>3B3AE017CBA407<br>E93F82421FA3 | A7E83056E9B3D9DDB1816B9<br>5518F6A5E5A1DFDFA28F605<br>33B1C850855EAA4263 |  |
| 7    | 1      | CN = Telia<br>Domain<br>Validation<br>CA v2<br>O = Telia<br>Finland Oyj<br>C = FI | TeliaSonera<br>Root CA v1 | 016584E34A38<br>D9E963EBEED<br>2174784         | RSA           | 4096<br>bits | sha256RSA        | 29 August<br>2018   | 18 October<br>2032  | ED3D749C2C53BB<br>71937B4B11F6B89<br>1E282F992DB | 5B312B7E11B70D07C14E0AB<br>99F08D00748966098C52AA85<br>A06A0822BBE59A02C |  |
| 8    | 1      | CN = Telia<br>Server CA<br>v3<br>O = Telia<br>Finland Oyj<br>C = FI               | Telia Root<br>CA v2       | 01675FE78F10<br>F349257F16B3<br>731F7A         | RSA           | 4096<br>bits | sha256RSA        | 29 November<br>2018 | 29 November<br>2043 | 46668D0E072316B<br>0EA4F05EB965AD<br>EA5EEC97EA4 | 1281AD8FABE883F209E96364<br>48D1A80C373DAA7686C813A<br>270FAD48F5F5E589A |  |
| 9    | 1      | CN =<br>TeliaSonera<br>Class 1 CA<br>v2<br>O =<br>TeliaSonera<br>C = FI           | TeliaSonera<br>Root CA v1 | 00FD41DD7FD<br>19F3EE9F85D<br>9E437133D4D<br>B | RSA           | 4096<br>bits | sha256RSA        | 16 October<br>2014  | 16 October<br>2032  | D147228FCBA85D<br>1AFE2641466ECB<br>824B657D8AE4 | B95AE54F838E3ABF0B57ACC<br>C1B1266DC68C7A3FA774015<br>FA128D60CDD1AAE280 |  |



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

| CA # | Cert # | Subject   | Issuer                    | Serial                                   | Key Algorithm | Key Size     | Digest Algorithm | Not Before         | Not After          | SKI  | SHA2 Fingerprint   | Other information |
|------|--------|---|---------------------------|--|---------------|--------------|------------------|--------------------|--------------------|--|--|-------------------|
| 10   | 1      | CN =<br>TeliaSonera<br>Class 2 CA<br>v2<br>O =<br>TeliaSonera<br>C = SE | TeliaSonera<br>Root CA v1 | 637C0BD785A<br>5BF29DA602D<br>7C4D7A70B1 | RSA           | 4096<br>bits | sha256RSA        | 16 October<br>2014 | 16 October<br>2032 | 9E19FFE50D3AFE<br>0097153F69F1DC5<br>A3CAA0C9483 | 092829433D231949F4A9BC66<br>6CBF54B3AA27D7BEBCA048<br>D75E59093E15A72EA5 |                   |
| 11   | 1      | CN =<br>TeliaSonera<br>Email CA<br>v4<br>O =<br>TeliaSonera<br>C = SE   | TeliaSonera<br>Root CA v1 | 52EBA0D8B74<br>B46EB8557CD<br>6DA2A3DDDD | RSA           | 4096<br>bits | sha256RSA        | 16 October<br>2014 | 16 October<br>2032 | 89862A82D178FAF<br>0A629543587956F<br>D3776019F0 | D1F2656AC8382739A3B087C<br>47AB5CAB945A32F162B6149<br>C308783C7E06AF8AE8 |                   |





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

## **Attachment B: Publicly disclosed incidents**

| # | Disclosure  | Publicly Disclosed Link              |
|---|---|--------------------------------------|
| 1 | Invalid email contact address was used for few domains              | <a href="#">Bugzilla Ticket Link</a> |
| 2 | Delayed revocation of 5 EE certificates in connection to id=1736020 | <a href="#">Bugzilla Ticket Link</a> |
| 3 | Issued three pre-certificates with non-NIST EC curve                | <a href="#">Bugzilla Ticket Link</a> |



## 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:

| # | Observation   | Relevant WebTrust Criteria   |
|---|---|--|
| 1 | <p>The Key Usage extension in the root CA certificates of <i>TeliaSonera Root CA v1</i> and <i>Sonera Class 2 CA</i> is not marked critical and <i>TeliaSonera Root CA v1</i> 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.</p> <p>However, Telia generated a new root CA, <i>Telia Root CA v2</i>, on 29 November 2018, which is planned to eventually replace <i>TeliaSonera Root CA v1</i> and <i>Sonera Class 2 CA</i>. 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.</p> | <p><b>Principle 2, Criteria 2.3</b></p> <p>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</p> |

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 practises 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 2021including 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 v2.5.

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:

| CA # | Cert # | Subject   | Issuer                 | Serial                             | Key Algorithm | Key Size  | Digest Algorithm | Not Before       | Not After        | SKI                                      | SHA2 Fingerprint   | Other information                              |
|------|--------|---|------------------------|------------------------------------|---------------|-----------|------------------|------------------|------------------|--|--|--|
| 1    | 1      | CN = TeliaSonera Root CA v1<br>O = TeliaSonera              | Self-signed            | 0095BE16A0F72E46F17B398272FA8BCD96 | RSA           | 4096 bits | sha1RSA          | 18 October 2007  | 18 October 2032  | F08F593800B3F58F9A960CD5EBFA7BAA17E81312 | DD6936FE21F8F077C123A1A521C12224F72255B73E03A7260693E8A24B0FA389 |  |
| 1    | 2      | CN = TeliaSonera Root CA v1<br>O = TeliaSonera              | Sonera Class2 CA       | 87ED2E1A28264AC519AA3AEBB90DA2CB   | RSA           | 4096 bits | sha256RSA        | 5 December 2014  | 5 April 2021     | F08F593800B3F58F9A960CD5EBFA7BAA17E81312 | E9563581E712B290F23A749346535EB0D981E3D4A39D56D604684CD0B1698C89 | Cross-certificate, Expired 5 April 2021        |
| 2    | 1      | CN = Sonera Class2 CA<br>O = Sonera<br>C = FI               | Self-signed            | 1D                                 | RSA           | 2048 bits | sha1RSA          | 16 April 2001    | 16 April 2021    | 4AA0AA5884D35E3C                         | 7908B40314C138100B518D0735807FFBFCF8518A0095337105BA386B153DD927 | Expired 16 April 2021                          |
| 3    | 1      | CN = Telia Root CA v2<br>O = Telia<br>Finland Oyj<br>C = FI | Self-signed            | 01675F27D6FE7AE3E4ACBE095B059E     | RSA           | 4096 bits | sha256RSA        | 29 November 2018 | 29 November 2043 | 72ACE43379AA4587F6FDAC1D9ED6C72F86D82439 | 242B69742FCB1E5B2ABF98898B94572187544E5B4D9911786573621F6A74B82C |  |
| 3    | 2      | CN = Telia Root CA v2<br>O = Telia<br>Finland Oyj<br>C = FI | TeliaSonera Root CA v1 | 01675F82BE0017DE8955A9376EB1F9     | RSA           | 4096 bits | sha256RSA        | 29 November 2018 | 18 October 2032  | 72ACE43379AA4587F6FDAC1D9ED6C72F86D82439 | EF6F29F636F62BDD4753122F41F3419EE7C2877587BE4A9807ADF58946458E7F | Cross-certificate                              |
| 4    | 1      | CN = TeliaSonera Server CA v2<br>O = TeliaSonera<br>C = FI  | TeliaSonera Root CA v1 | 4C462AF6DBFBF7804F84C17CFEA972B6   | RSA           | 4096 bits | sha256RSA        | 16 October 2014  | 16 October 2032  | 2F493C294FD70725F9C68CD564F5663D12832295 | D721110388CA6F20BBA9FD1A8DBA4EFB8C16392A3DEBAD97C553EEAF0ACACAAC |  |
| 5    | 1      | CN = TeliaSonera Gateway CA v2<br>O = TeliaSonera<br>C = FI | TeliaSonera Root CA v1 | 00863C75641195854FB43138A0A0CF8AA3 | RSA           | 4096 bits | sha256RSA        | 16 October 2014  | 16 October 2032  | 87AAE313129F118BCA68CD1E2DC429A8FA101ACB | 46226B7B89E02CA8F5D85D67ED8CB4B19C48382058BB16242199D540CABE9268 | Revoked (Cessation Of Operation) 28 April 2021 |
| 6    | 1      | CN = Telia Domain Validation CA v3                          | Telia Root CA v2       | 01675FFDE7E41811E2CD76B0CDB50A     | RSA           | 4096 bits | sha256RSA        | 29 November 2018 | 29 November 2043 | 5BF1EE298D31B23B3AE017CBA407E93F82421FA3 | A7E83056E9B3D9DDB1816B95518F6A5E5A1DFDFA28F60533B1C850855EAA4263 |  |



| CA # | Cert # | Subject   | Issuer                 | Serial   | Key Algorithm | Key Size  | Digest Algorithm | Not Before       | Not After        | SKI  | SHA2 Fingerprint   | Other information |
|------|--------|---|------------------------|--|---------------|-----------|------------------|------------------|------------------|--|--|-------------------|
|      |        | O = Telia<br>Finland Oyj<br>C = FI                                    |                        |  |               |           |                  |                  |                  |  |  |                   |
| 7    | 1      | CN = Telia Domain Validation CA v2<br>O = Telia Finland Oyj<br>C = FI | TeliaSonera Root CA v1 | 016584E34A38<br>D9E963EBEED<br>2174784         | RSA           | 4096 bits | sha256RSA        | 29 August 2018   | 18 October 2032  | ED3D749C2C53BB<br>71937B4B11F6B89<br>1E282F992DB | 5B312B7E11B70D07C<br>14E0AB99F08D007489<br>66098C52AA85A06A08<br>22BBE59A02C |                   |
| 8    | 1      | CN = Telia Server CA v3<br>O = Telia Finland Oyj<br>C = FI            | Telia Root CA v2       | 01675FE78F10<br>F349257F16B3<br>731F7A         | RSA           | 4096 bits | sha256RSA        | 29 November 2018 | 29 November 2043 | 46668D0E072316B<br>0EA4F05EB965AD<br>EA5EEC97EA4 | 1281AD8FABE883F20<br>9E9636448D1A80C373<br>DAA7686C813A270FA<br>D48F5F5E589A |                   |
| 9    | 1      | CN = TeliaSonera Class 1 CA v2<br>O = TeliaSonera<br>C = FI           | TeliaSonera Root CA v1 | 00FD41DD7FD<br>19F3EE9F85D<br>9E437133D4D<br>B | RSA           | 4096 bits | sha256RSA        | 16 October 2014  | 16 October 2032  | D147228FCBA85D<br>1AFE2641466ECB<br>824B657D8AE4 | B95AE54F838E3ABF0<br>B57ACCC1B1266DC68<br>C7A3FA774015FA128<br>D60CDD1AAE280 |                   |
| 10   | 1      | CN = TeliaSonera Class 2 CA v2<br>O = TeliaSonera<br>C = SE           | TeliaSonera Root CA v1 | 637C0BD785A<br>5BF29DA602D<br>7C4D7A70B1       | RSA           | 4096 bits | sha256RSA        | 16 October 2014  | 16 October 2032  | 9E19FFE50D3AFE<br>0097153F69F1DC5<br>A3CAA0C9483 | 092829433D231949F4<br>A9BC666CBF54B3AA2<br>7D7BEBCA048D75E59<br>093E15A72EA5 |                   |
| 11   | 1      | CN = TeliaSonera Email CA v4<br>O = TeliaSonera<br>C = SE             | TeliaSonera Root CA v1 | 52EBA0D8B74<br>B46EB8557CD<br>6DA2A3DDDD       | RSA           | 4096 bits | sha256RSA        | 16 October 2014  | 16 October 2032  | 89862A82D178FAF<br>0A629543587956F<br>D3776019F0 | D1F2656AC8382739A3<br>B087C47AB5CAB945A<br>32F162B6149C308783<br>C7E06AF8AE8 |                   |



## Attachment B: Publicly disclosed incidents

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