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 business, key life cycle management, certificate life cycle management, and CA environmental control 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

► maintained effective controls to provide reasonable assurance that
  - Telia provides its services in accordance with its Certification Practice Statements

► maintained effective controls to provide reasonable assurance that
  - the integrity of keys and certificates it manages is established and protected throughout their life cycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;
  - subscriber information is properly authenticated (for the registration activities performed by Telia); and
  - subordinate CA certificate requests are accurate, authenticated, and approved

► 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v.2.0.

Telia makes use of external registration authorities for specific subscriber registration activities as disclosed in Telia's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.

Telia does not have separate Certificate Policy documents, does not escrow its CA keys, does not provide integrated circuit card (ICC) life cycle management services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.
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 v2.0.

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 key and certificate life cycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate life cycle management operations and over development, maintenance and operation of systems integrity;
2. selectively testing transactions executed in accordance with disclosed key and certificate life cycle 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’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.

---

\(^1\) ISQC 1, Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements
Basis for qualified opinion

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

<table>
<thead>
<tr>
<th>#</th>
<th>Deviation</th>
<th>Relevant WebTrust Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The CA had not prepared and followed a key generation script for the key generation ceremonies of Telia Domain Validation SSL CA v1 and Telia Document Signing CA v1 issuing CAs. This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 4.1 to not be met.</td>
<td>4.1 CA Key Generation</td>
</tr>
</tbody>
</table>

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 business, key life cycle management, certificate life cycle management, and CA environmental control 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
► maintained effective controls to provide reasonable assurance that
   - Telia provides its services in accordance with its Certification Practice Statements

► maintained effective controls to provide reasonable assurance that
   - the integrity of keys and certificates it manages is established and protected throughout their life cycles;
   - the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;
   - subscriber information is properly authenticated (for the registration activities performed by Telia); and
   - subordinate CA certificate requests are accurate, authenticated, and approved

► 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.0.
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 v2.0, 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

Júha Sunila
Senior Manager, CISA, CISSP
## Attachment A: List of CAs in Scope

The following CAs were in the 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 and Size</th>
<th>Digest Algorithm</th>
<th>Not Before</th>
<th>Not After</th>
<th>Subject Key Identifier</th>
<th>SHA1 Fingerprint</th>
<th>Other Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>CN = Sonera Class2 CA O = Sonera C = FI</td>
<td>Self-signed</td>
<td>1d</td>
<td>RSA 2048 bits</td>
<td>sha1RSA</td>
<td>6 April 2001</td>
<td>6 April 2021</td>
<td>4a a0 aa 58 84 d3 5e 3c</td>
<td>37 1f 6d e6 07 7c 90 c5 b1 3e 93 1a b7 41 10 b4 f2 e4 9a 27</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>CN = TeliaSonera Root CA v1 O = TeliaSonera</td>
<td>Self-signed</td>
<td>00 95 be 16 a0 f7 2e 46 f1 7b 39 82 72 a8 b0 cd 96</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>18 October 2007</td>
<td>18 October 2032</td>
<td>0f 8f 59 38 00 b3 f5 8f 9a 96 0c d5 eb fa 7b aa 17 e8 13 12</td>
<td>43 13 bb 96 1f d5 86 9b c1 4e 6a 92 16 cf f6 34 69 87 82 37</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>CN = TeliaSonera Root CA v1 O = TeliaSonera</td>
<td>Sonera Class2 CA</td>
<td>00 87 ed 2e 1a 28 26 4a c5 19 aa 3a eb b9 0d a2 cb</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>5 December 2014</td>
<td>5 April 2021</td>
<td>0f 8f 59 38 00 b3 f5 8f 9a 96 0c d5 eb fa 7b aa 17 e8 13 12</td>
<td>49 3c 6c c9 3a 44</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>CN = TeliaSonera Root CA v1 O = TeliaSonera</td>
<td>Sonera Class2 CA</td>
<td>00 d1 e0 3e 5b 48 ed c7 9e 09 3f 40 de e1 61 c3 8b</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>18 October 2007</td>
<td>17 October 2019</td>
<td>0f 8f 59 38 00 b3 f5 8f 9a 96 0c d5 eb fa 7b aa 17 e8 13 12</td>
<td>4f 67 16 71 48 8b c8 34 66 38 88 a6 9a 4b 4c 99 74 16 d6 06</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>CN = TeliaSonera Extended Validation SSL CA v1 O = TeliaSonera C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>00 99 38 b8 d6 06 28 ea 59 2e 26 01 0f d2 66 e8 11</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 March 2015</td>
<td>17 October 2032</td>
<td>08 e4 fa 72 d5 43 3b c2 5c 24 9b 95 92 40 f3 d0 9f 7a a8 30</td>
<td>11 f5 48 b0 1e b2 66 fa 95 c3 0f 79 c3 c9 15 58 ea 3d f1 8c</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>4c 46 2a 16 db fb f7 80 4f 84 1c 7c fe a9 72 b6</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>2f 49 3c 29 4f d7 07 25 f9 c6 8c d5 f4 15 66 3d 12 83 22 95</td>
<td>0e c6 42 d0 0f 8d cf 7b 19 6a c0 a9 12 c8 57 e3 42 68 79 4a</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>CN = TeliaSonera Server CA v1 O = TeliaSonera</td>
<td>TeliaSonera Root CA v1</td>
<td>10 68 4a 0d 86 e8 43 59 2d 16 74 6a 88 15 2f 81</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>13 May 2013</td>
<td>17 October 2032</td>
<td>a0 81 be 55 9b 13 f1 61 05 84 8b 2d 0c 3b e0 08 49 ee 57 3e</td>
<td>41 c4 34 fa 80 ed b4 bf 58 a6 98 c2 b1 54 20 d6 f3 4a 33 d0</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>CN = TeliaSonera Gateway CA v2 O = TeliaSonera C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>00 86 3c 75 64 11 95 85 4f b4 31 38 a0 a0 cf 8a a3</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>87 aa e3 13 12 9f 11 8b ca 68 cd 1e 2d c4 29 a8 fa 10 1a cb</td>
<td>3f 1a 1c cb eb b8 c7 3b e9 94 46 91 8e 3f af f3 ae d2 47 a3</td>
<td></td>
</tr>
<tr>
<td>CA #</td>
<td>Cert. Subject</td>
<td>Issuer</td>
<td>Serial</td>
<td>Key Algorithm and Size</td>
<td>Digest Algorithm</td>
<td>Not Before</td>
<td>Not After</td>
<td>Subject Key Identifier</td>
<td>SHA1 Fingerprint</td>
<td>Other Information</td>
<td></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>7</td>
<td>CN = TeliaSonera Gateway CA v1 O = TeliaSonera Root CA v1</td>
<td>TeliaSonera Root CA v1</td>
<td>35 79 1d 87 92 51 6d 61 b1 1c 4b ef af 76 c1 da</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>13 May 2013</td>
<td>17 October 2032</td>
<td>8f 59 95 28 26 a2 b0 6d 19 49 99 d2 fb b0 84 47 4d cb 95 fc</td>
<td>0d e2 60 1f 7f 96 5c c7 d1 cc be 92 21 26 68 52 9f e5 5f 7d cd</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>CN = Telia Domain Validation SSL CA v1 O = Telia Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>01 61 ae 20 05 ce 3f 12 7e f8 8d d7 25 1b b1</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>19 February 2018</td>
<td>16 October 2032</td>
<td>49 6c 32 53 7c 5d ed 2b e3 a2 ab 9c 0b c9 5d e4 95 d4 92 5f</td>
<td>8e 16 4d f8 80 51 da 37 8a 68 d8 f4 01 87 6d 29 c1 c7 7c 5b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>CN = Telia Document Signing CA v1 O = Telia Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>01 60 4b 22 16 76 3f 09 01 ee 04 83 6b 97 3c</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>28 November 2017</td>
<td>18 October 2032</td>
<td>ee 2a a3 20 42 d6 99 4e 4e 3d 1e 9e 4f e0 b8 a9 9d 74 db fa</td>
<td>59 51 61 ab 72 81 54 58 7b 6f 38 ad 93 6c c0 3a b1 2b 8f 90</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>CN = TeliaSonera Class 1 CA v2 O = TeliaSonera C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>00 1d 41 dd 71 d1 9f 3e 9f f8 5d 9e 43 71 33 d4 db</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>d1 47 22 8f cb a8 5d 1a fe 26 41 46 6e cb 82 4b 65 7d 8a e4</td>
<td>89 e3 c8 68 96 af 10 e2 f4 ee cb c8 12 04 6b b9 a4 4c 8f d0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>CN = TeliaSonera Class 1 CA v1 O = TeliaSonera</td>
<td>TeliaSonera Root CA v1</td>
<td>00 18 5d 21 19 0c 60 9f 14 94 b2 8d f9 c1 d1 e7 4c</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>13 May 2013</td>
<td>17 October 2032</td>
<td>f5 ea 33 8c i8 a5 2e 8c a6 82 6b 4d b3 32 2a a7 b7 53 cf cc</td>
<td>6c 0d 9c 40 94 9c 7e a5 72 a5 b9 48 01 98 8a 9f 19 b4 07 e9</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>CN = TeliaSonera Class 2 CA v2 O = TeliaSonera C = SE</td>
<td>TeliaSonera Root CA v1</td>
<td>63 7c 0b d7 85 a5 bf 29 da 60 2d 7c 4d 7a 70 b1</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>9e 19 ff e5 0d 3a fe 00 97 15 3f 69 f1 dc 5a 3c aa 0c 94 83</td>
<td>25 a6 d3 e3 86 59 63 cf 5a d9 7b 31 2a 26 86 e2 4e db 92 24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>CN = TeliaSonera Class 2 CA v1 O = TeliaSonera</td>
<td>TeliaSonera Root CA v1</td>
<td>00 d0 d7 72 72 9a 04 17 9f 18 9e da e3 82 f9 11 11</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>13 May 2013</td>
<td>17 October 2032</td>
<td>d4 6d bd b2 55 bb 52 4b 2a e6 b3 df 6d a7 d8 01 fb 67 9f 72</td>
<td>51 e6 35 0e 44 5c 1f 7c ca a2 7d 5b 6b a2 1d 28 65 ae 04 a4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>CN = TeliaSonera Email CA v4 O = TeliaSonera C = SE</td>
<td>TeliaSonera Root CA v1</td>
<td>52 eb a0 d8 b7 4b 46 eb 85 57 cd 6d a2 a3 dd dd</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>89 86 2a 82 d1 78 fa f0 a6 29 54 35 87 95 6f d3 77 60 19 f0</td>
<td>df fd 4e cf 7f c0 17 0a 53 bd eb ea 18 20 fb 4f 95 04 60 f5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA Cert. Subject</td>
<td>Issuer</td>
<td>Serial</td>
<td>Key Algorithm and Size</td>
<td>Digest Algorithm</td>
<td>Not Before</td>
<td>Not After</td>
<td>Subject Key Identifier</td>
<td>SHA1 Fingerprint</td>
<td>Other Information</td>
<td></td>
<td></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>15 1 CN = TeliaSonera Email CA v3 O = TeliaSonera</td>
<td>TeliaSonera Root CA v1 00 81 51 ad 72 8b 67 a5 7f a4 55 24 8d 81 d3 57 f9</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>13 May 2013</td>
<td>17 October 2032</td>
<td>TeliaSonera Email CA v3</td>
<td>1c 7b 19 9e 97 9c 76 6a e3 db 2d a6 53</td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16 1 CN = Ericsson NL Individual CA v3 O = Ericsson C = SE</td>
<td>TeliaSonera Root CA v1 53 b8 7e 83 e1 9c 99 28 93 b0 9b 49 1c ec b8 eb</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>27 October 2015</td>
<td>27 October 2025</td>
<td>Ericsson NL Individual CA v3</td>
<td>15 4f 51 15 8e 62 15 8f 5b 01</td>
<td>The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-emailProtection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17 1 CN = Ericsson NL Individual CA v2 O = Ericsson</td>
<td>TeliaSonera Root CA v1 00 a0 0c cb cc 9b 99 98 ec e2 3a 70 f4 7c c1 c0 59</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>27 May 2014</td>
<td>27 May 2024</td>
<td>Ericsson NL Individual CA v2</td>
<td>27 45 1f a5 c9 1d aa b6 ee 4e 2e b1 e5 49 07 3f</td>
<td>The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-emailProtection</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>CA #</th>
<th>Cert. #</th>
<th>Subject</th>
<th>Issuer</th>
<th>Serial</th>
<th>Key Algorithm and Size</th>
<th>Digest Algorithm</th>
<th>Not Before</th>
<th>Not After</th>
<th>Subject Key Identifier</th>
<th>SHA1 Fingerprint</th>
<th>Other Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>1</td>
<td>CN = TeliaSonera Mobile ID CA v2 O = TeliaSonera Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>01 61 ae 3e 89 33 e5 b8 95 8a ef 92 8c 0c eb</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>19 February 2018</td>
<td>17 October 2032</td>
<td>d0 2d d3 14 f0 77 4a 62 27 2c 65 53 93 d5 a5 a5 43 af c2 52</td>
<td>16 6a 7f a3 71 eb 9f 97 ca 27 ae 04 0b</td>
<td>The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-timeStamping</td>
</tr>
<tr>
<td>2</td>
<td>CN = TeliaSonera Mobile ID CA v2 O = TeliaSonera Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>03 75 c4 9b 7e 63 ce 43 37 07 ff 19 84 37 a5 ef</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>26 January 2016</td>
<td>17 October 2032</td>
<td>d0 2d d3 14 f0 77 4a 62 27 2c 65 53 93 d5 a5 a5 43 af c2 52</td>
<td>57 b2 20 23 1d c6 b6 9c a5 0a cc c9 bc 66 b0 84 9b aa 78 2a</td>
<td>The certificate has been revoked 17 Apr 2018. The CA certificate had the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-timeStamping</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>1</td>
<td>CN = TeliaSonera Mobile ID CA v1 O = TeliaSonera Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>01 63 8b ea 73 4a fa 18 71 6e 51 24 37 11 72</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>23 May 2018</td>
<td>16 October 2032</td>
<td>53 80 2c e5 18 4b 1e c1 db d6 26 2c d1 08 ef 88 86 dd 2c 0e</td>
<td>68 a5 35 9c a1 c7 72 33 ca 27 66 3f 1d 29 7e e8 43 62 a1 22</td>
<td>The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth</td>
</tr>
<tr>
<td>2</td>
<td>CN = TeliaSonera Mobile ID CA v1 O = Telia Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>01 62 a1 14 90 9a 4c 15 5a 56 ba 6d b7 ab 5f</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>10 April 2018</td>
<td>16 October 2032</td>
<td>53 80 2c e5 18 4b 1e c1 db d6 26 2c d1 08 ef 88 86 dd 2c 0e</td>
<td>90 ef e8 0c da 70 af 07 10 93 8f c6 a9 d0 60 9c 0c f4 4a ba</td>
<td>The certificate has been revoked 23 May 2018. The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>CN = TeliaSonera Mobile ID CA v1 O = TeliaSonera Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>00 d7 6a 8b c5 05 09 00 a1 9b 44 5c 87 28 cc aa 36</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>53 80 2c e5 18 4b 1e c1 db d6 26 2c d1 08 ef 88 86 dd 2c 0e</td>
<td>80 2f f3 13 f0 b8 b6 26 36 35 c2 fc a6 6a 20 c3 df ff fd 6a 19</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>CN = TeliaSonera Mobile ID CA v1 O = TeliaSonera Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>00 19 4c 94 77 c4 fb 88 be 33 5e 65 72 d3 7a 72 25</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 December 2010</td>
<td>17 October 2032</td>
<td>53 80 2c e5 18 4b 1e c1 db d6 26 2c d1 08 ef 88 86 dd 2c 0e</td>
<td>cb 18 ac 54 e8 d1 6c 01 93 dd 95 4e 18 53 7b 8a 71 b2 34 e7</td>
<td>The certificate has been revoked 23 May 2018. The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-emailProtection</td>
<td></td>
</tr>
</tbody>
</table>
TELIA’S MANAGEMENT STATEMENT

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

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management
- Subordinate CA certification

The management of Telia is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key life cycle management controls, subscriber key life cycle management controls, certificate life cycle management controls, and subordinate CA certificate life cycle management controls. These controls contain monitoring mechanisms, and actions to be taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to Telia’s Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Telia management has assessed its disclosures of its certificate practices and controls over its 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>Deviation</th>
<th>Relevant WebTrust Criteria</th>
</tr>
</thead>
</table>
| 1  | The CA had not prepared and followed a key generation script for the key generation ceremonies of Telia Domain Validation SSL CA v1 and Telia Document Signing CA v1 issuing CAs. This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 4.1 to not be met. | 4.1 CA Key Generation
The CA maintains controls to provide reasonable assurance that CA key pairs are generated in accordance with the CA's disclosed business practices and defined procedures specified within detailed key generation ceremony scripts.
The CA's disclosed business practices include but are not limited to:
a) generation of CA keys are undertaken in a physically secured environment (see §3.4);
b) generation of CA keys are performed by personnel in trusted roles (see §3.3) under the principles of multiple person control and split knowledge;
c) generation of CA keys occur within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's CPS;
d) generation of CA keys are witnessed by an independent party and/or videotaped; and
e) CA key generation activities are logged.
The CA key generation script includes the following:
a) definition of roles and participant responsibilities;
b) approval for conduct of the key generation ceremony;
c) cryptographic hardware and activation materials required for the ceremony; |
Based on that assessment, in Telia management’s opinion, except for the matters described in the preceding table, in providing its Certification Authority (CA) services in Finland and Sweden, throughout the period 1 April 2017 to 31 March 2018, Telia has:

- disclosed its business, key life cycle management, certificate life cycle management, and CA environmental control 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

- maintained effective controls to provide reasonable assurance that
  - Telia provides its services in accordance with its Certification Practice Statements

- maintained effective controls to provide reasonable assurance that
  - the integrity of keys and certificates it managed is established and protected throughout their life cycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;
  - subscriber information is properly authenticated (for the registration activities performed by Telia); and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v.2.0 including the following:

**CA Business Practices Disclosure**
- Certification Practice Statement (CPS)

**CA Business Practices Management**
- Certification Practice Statement Management
CA Environmental Controls
- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Life Cycle Management Controls
- CA Key Generation
- CA Key Storage, Backup and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management

Subscriber Key Life Cycle Management Controls
- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Requirements for Subscriber Key Management

Certificate Life Cycle Management Controls
- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Life Cycle Management Controls
- Subordinate CA Certificate Life Cycle Management

Telia does not have separate Certificate Policy documents, does not escrow its CA keys, does not provide integrated circuit card (ICC) life cycle management services, and does not provide certificate suspension services. Accordingly, our statement does not extend to controls that would address those criteria.

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 the scope of the assessment:

<table>
<thead>
<tr>
<th>CA #</th>
<th>Cert #</th>
<th>Subject</th>
<th>Issuer</th>
<th>Serial</th>
<th>Key Algorithm and Size</th>
<th>Digest Algorithm</th>
<th>Not Before</th>
<th>Not After</th>
<th>Subject Key Identifier</th>
<th>SHA1 Fingerprint</th>
<th>Extended Key Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>CN = Sonera Class2 CA O = Sonera C = FI</td>
<td>Self-signed</td>
<td>1d</td>
<td>RSA 2048 bits</td>
<td>sha1RSA</td>
<td>6 April 2001</td>
<td>6 April 2021</td>
<td>4a a0 aa 58 84 d3 5e 3c</td>
<td>37 17 6d e6 07 7c 90 c5 b1 3e 93 1a b7 41 10 b4 f2 e4 9a 27</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>CN = TeliaSonera Root CA v1 O = TeliaSonera</td>
<td>Self-signed</td>
<td>00 95 be 16 a0 f7 2e 46 f1 7b 39 82 72 fa 8b cd 96</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>18 October 2007</td>
<td>18 October 2032</td>
<td>f0 8f 59 38 00 b3 f5 8f 9a 96 0c d5 eb fa 7b aa 17 e8 13 12</td>
<td>43 13 bb 96 f1 d5 86 9b c1 4e 6a 92 f6 cf f6 34 69 87 82 37</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>CN = TeliaSonera Root CA v1 O = TeliaSonera</td>
<td>Sonera Class2 CA</td>
<td>00 87 be 2e 1a 28 26 4a c5 19 aa 3a eb b9 0d a2 cb</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>5 December 2014</td>
<td>5 April 2021</td>
<td>f0 8f 59 38 00 b3 f5 8f 9a 96 0c d5 eb fa 7b aa 17 e8 13 12</td>
<td>9f 6f 1d eb b4 ed 26 3b 4d be c7 79 87 ca 49 3c 6c c9 3a a4</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>CN = TeliaSonera Root CA v1 O = TeliaSonera</td>
<td>Sonera Class2 CA</td>
<td>00 d1 e0 3e 5b 48 ed c7 9e 09 3f 40 de e1 61 c3 8b</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>18 October 2007</td>
<td>17 October 2019</td>
<td>f0 8f 59 38 00 b3 f5 8f 9a 96 0c d5 eb fa 7b aa 17 e8 13 12</td>
<td>44 67 16 71 48 8b c8 34 66 38 88 a6 9a db 4c b9 74 16 d8 06</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>CN = TeliaSonera Extended Validation SSL CA v1 O = TeliaSonera C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>00 99 38 bb d6 06 28 ea 59 2e 26 01 0f d2 66 e8 11</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 March 2015</td>
<td>17 October 2032</td>
<td>08 e4 fa 72 d5 43 3b c2 5c 24 9b 95 92 40 f3 d0 9f 7a a8 30</td>
<td>f1 55 48 b0 1e b2 66 fa 95 c3 0f 79 c3 c9 1f 58 ea 3d f1 8c</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>4c 46 2a f6 db fb f7 80 4f 84 c1 7c fe a9 72 b6</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>2f 49 3c 29 4f d7 07 25 f9 c8 5c d5 64 f5 66 3d 12 83 22 95</td>
<td>0e c6 42 d0 0f d6 cb 19 6a c0 a9 f2 c8 57 e3 42 68 79 a4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>CN = TeliaSonera Server CA v1 O = TeliaSonera</td>
<td>TeliaSonera Root CA v1</td>
<td>10 88 4a 0d 86 e8 43 59 2d 16 74 6a 88 15 2f 51</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>13 May 2013</td>
<td>17 October 2032</td>
<td>a0 81 be 95 9b 13 f7 61 05 84 8b 2d 0c 3b e0 88 49 ee 57 e6</td>
<td>41 c4 34 fa 80 ed b4 bf 5b 8e c2 b1 54 20 d6 f3 4a 33 d0</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>CN = TeliaSonera Gateway CA v2 O = TeliaSonera C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>00 86 5c 75 64 11 95 85 4f b1 31 38 a0 a0 cf 8a a3</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>87 aa e3 13 12 9f 11 8b 6a 68 cd 1e 2d c4 29 a8 fa 10 1a cb</td>
<td>3f 1a 1c cb eb b8 c7 3b e9 94 46 91 8e 3f af f3 ae d2 47 a3</td>
<td></td>
</tr>
</tbody>
</table>

The CA did not issue certificates during the period 1 April 2017 to 31 Mar 2018 and was maintained online to provide revocation status information only.
<table>
<thead>
<tr>
<th>CA #</th>
<th>Cert. #</th>
<th>Subject</th>
<th>Issuer</th>
<th>Serial</th>
<th>Key Algorithm and Size</th>
<th>Digest Algorithm</th>
<th>Not Before</th>
<th>Not After</th>
<th>Subject Key Identifier</th>
<th>SHA1 Fingerprint</th>
<th>Extended Key Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>1</td>
<td>CN = TeliaSonera Gateway CA v1 O = TeliaSonera Root CA v1</td>
<td>TeliaSonera Root CA v1</td>
<td>35 79 1d 87 92 51 6d b1 1c 4b e8 af 76 c1 da</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>13 May 2013</td>
<td>17 October 2032</td>
<td>8f 59 95 28 26 a2 b0 6d 19 49 99 d2 fb b0 94 47 4d cb 95 fc</td>
<td>0d e2 60 17 96 5c c7</td>
<td>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.</td>
</tr>
<tr>
<td>8</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>01 61 ae 20 05 ce 3f 12 7e e8 8d d7 25 1b b1</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>19 February 2018</td>
<td>16 October 2032</td>
<td>49 6c 32 53 7c 5d ed 2b e3 a2 ab 9c 0b c9 5d e4 95 d4 92 5f</td>
<td>8e 16 4d 8f 80 51 da 37 8a 68 d8 01 87 6d 29 c1 c7 7c 5b</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>CN = Telia Document Signing CA v1 O = Telia Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>00 60 4b 22 1f 76 3f 09 01 ee 04 83 6b 97 3c</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>28 November 2017</td>
<td>18 October 2032</td>
<td>ee 2a a3 20 42 d6 99 4e 4e 3d 1e 9e 4f e0 0b 0a 9d 74 db fa</td>
<td>59 51 61 ab 72 81 54 58 76 3f 38 ad 93 6c c0 3a b1 2b 8f 90</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>CN = TeliaSonera Class 1 CA v2 O = TeliaSonera C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>00 6d 41 df 7f d1 9f 3e e9 f8 5d 9e 43 71 33 df db</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>d1 47 22 8f cb a8 5d 1a te 2e 26 41 46 6e cb 82 4f 65 7d 8a e4</td>
<td>89 e3 c8 68 96 af 10 e2 4e ee cb c8 12 04 6e b9 a4 4c 8f df</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>CN = TeliaSonera Class 1 CA v1 O = TeliaSonera</td>
<td>TeliaSonera Root CA v1</td>
<td>00 18 5d 2f 19 0c 60 9f 14 94 b2 9d f9 c1 d1 e7 4c</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>13 May 2013</td>
<td>17 October 2032</td>
<td>f6 ea 33 8c f8 a5 2e 8c ae 82 60 4d 8b 23 2a a7 b7 53 cf cc</td>
<td>6d 0f 9c 40 94 9c 7e a5 72 a5 b6 48 01 98 8a 9f 19 b4 07 e9</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>CN = TeliaSonera Class 2 CA v2 O = TeliaSonera C = SE</td>
<td>TeliaSonera Root CA v1</td>
<td>63 7c 0b d7 85 a5 bf 29 da 6b 2d 7c 4d 7a 70 b1</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>9e 19 ff e5 0d 3a fe 00 97 15 3f 6f 1f dc 5a 3c aa 0c 94 83</td>
<td>25 5a d6 e3 86 59 63 cf 5a df 7b 31 2a 26 86 e2 4e db 92 24</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>CN = TeliaSonera Class 2 CA v1 O = TeliaSonera</td>
<td>TeliaSonera Root CA v1</td>
<td>00 d0 df 77 72 9a 04 17 97 8f 9e da e3 82 f9 1f 11</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>13 May 2013</td>
<td>17 October 2032</td>
<td>d4 6d b2 5b bb 52 4b 2a e8 b3 df 6d a7 db 01 fb 6f 7f 72</td>
<td>51 e6 35 0e 44 5c 11 7c ca a2 7d 5b 6b a2 1d 28 65 ae 04 a4</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>1</td>
<td>CN = TeliaSonera Email CA v4 O = TeliaSonera C = SE</td>
<td>TeliaSonera Root CA v1</td>
<td>52 eb a0 db 7b 4b 46 eb 85 57 cd 6d a2 a3 dd dd</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>89 86 2a 82 d1 78 fa f0 a6 29 54 35 87 95 6f d3 77 60 19 f0</td>
<td>df fd 4e 47 cf 17 0a 53 db ea 18 20 2b 4f 95 04 60 15</td>
<td></td>
</tr>
</tbody>
</table>
### TELIA CERTIFICATION AUTHORITY

<table>
<thead>
<tr>
<th>CA #</th>
<th>Cert. #</th>
<th>Subject</th>
<th>Issuer</th>
<th>Serial</th>
<th>Key Algorithm and Size</th>
<th>Digest Algorithm</th>
<th>Not Before</th>
<th>Not After</th>
<th>Subject Key Identifier</th>
<th>SHA1 Fingerprint</th>
<th>Extended Key Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>1</td>
<td>CN = TeliaSonera Email CA v3 O = TeliaSonera</td>
<td>TeliaSonera Root CA v1</td>
<td>00 81 51 ad 72 8b 67 a5 7f a4 55 24 8d 61 d3 57 f9</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>13 May 2013</td>
<td>17 October 2032</td>
<td>f3 74 b8 1d 13 33 d1 c9 ad 5b ce 66 28 9a 99 32 81 f0 20 ce</td>
<td>11 ef 59 16 40 5e 41 0d 0c 7f 43 36 f9 11 90 16 ed 62 96 29</td>
<td>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.</td>
</tr>
<tr>
<td>16</td>
<td>1</td>
<td>CN = Ericsson NL Individual CA v3 O = Ericsson C = SE</td>
<td>TeliaSonera Root CA v1</td>
<td>53 b8 7e 83 e1 9c 99 28 93 b0 9b 49 1c ec b8 eb</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>27 October 2015</td>
<td>27 October 2025</td>
<td>1c 7b 19 9e 97 9c 76 ac 20 3d d8 dc e3 91 6a e3 db 2d a6 53</td>
<td>1f d9 4b dd 46 fe 6f 7b 3b 29 d0 b3 a4 37 fd 47 96 65 4d e5</td>
<td>The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-emailProtection</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>CN = Ericsson NL Individual CA v2 O = Ericsson</td>
<td>TeliaSonera Root CA v1</td>
<td>00 a0 0c cb cc 9b 99 98 ec e2 3a 70 14 7c c1 c0 59</td>
<td>RSA 4096 bits</td>
<td>sha1RSA</td>
<td>27 May 2014</td>
<td>27 May 2024</td>
<td>b1 0d ca da 46 b7 af 86 02 c3 2f 61 06 ca 0e 76 71 71 4b 37</td>
<td>27 45 1f a5 c9 1d aa bf e4 2e b1 a5 49 07 df 32 a5 b1 58 b0</td>
<td>The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-emailProtection</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>CA #</th>
<th>Cert. #</th>
<th>Subject</th>
<th>Issuer</th>
<th>Serial</th>
<th>Key Algorithm and Size</th>
<th>Digest Algorithm</th>
<th>Not Before</th>
<th>Not After</th>
<th>Subject Key Identifier</th>
<th>SHA1 Fingerprint</th>
<th>Other information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>CN = TeliaSonera Mobile ID CA v2 O = TeliaSonera Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>01 61 ae 3e 89 33 e5 b8 95 8a ef 92 9c 0c eb</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>19 February 2018</td>
<td>17 October 2032</td>
<td>d0 2d d3 14 10 77 4a 62 27 2c 65 53 93 d5 a5 a5 43 af c2 52</td>
<td>16 6a 71 a3 71 eb 9f 97 87 ea b2 69 88 a0 98 ca 27 a8 04 0b</td>
<td>The CA certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth id-kp-timeStamping</td>
</tr>
</tbody>
</table>
## TELIA CERTIFICATION AUTHORITY

<table>
<thead>
<tr>
<th>CA #</th>
<th>Cert. #</th>
<th>Subject</th>
<th>Issuer</th>
<th>Serial</th>
<th>Key Algorithm and Size</th>
<th>Digest Algorithm</th>
<th>Not Before</th>
<th>Not After</th>
<th>Subject Key Identifier</th>
<th>SHA1 Fingerprint</th>
<th>Other information</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>CN = TeliaSonera Mobile ID CA v2 O = TeliaSonera Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>03 75 c4 9b 7e 63 ce 43 37 07 ff 19 84 37 a5 ef</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>26 January 2016</td>
<td>17 October 2032</td>
<td>03 63 8b ea 73 4a fa f8 71 6e 51 24 37 11 72</td>
<td>57 b2 20 23 1d c6 b6 9c a5 0a cc c9 bc 66 b0 84 9b aa 78 2a</td>
<td>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</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>CN = TeliaSonera Mobile ID CA v1 O = TeliaSonera Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>01 63 8b ea 73 4a fa f8 71 6e 51 24 37 11 72</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>23 May 2018</td>
<td>16 October 2032</td>
<td>53 80 2c e5 18 4b 1e c1 0b d6 26 2c d1 08 ef 88 86 dd 2c 0e</td>
<td>68 a5 35 9c a1 c7 72 33 ca 27 66 3f 1d 29 7e e8 43 62 a1 22</td>
<td>The certificate has the following Extended Key Usage (EKU) attributes: id-kp-clientAuth</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>CN = TeliaSonera Mobile ID CA v1 O = TeliaSonera Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>00 d7 6a 8b c5 05 09 00 a1 9b 44 5c 87 28 cc a6 36</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 October 2014</td>
<td>16 October 2032</td>
<td>53 80 2c e5 18 4b 1e c1 0b d6 26 2c d1 08 ef 88 86 dd 2c 0e</td>
<td>80 2f 13 0f b8 b6 26 63 35 c2 fc a8 6e 20 c3 df ff fd 6a 19</td>
<td>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</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>CN = TeliaSonera Mobile ID CA v1 O = TeliaSonera Finland Oyj C = FI</td>
<td>TeliaSonera Root CA v1</td>
<td>00 f9 4c 94 77 c4 fb 88 be 33 5e 65 72 d3 7a 72 25</td>
<td>RSA 4096 bits</td>
<td>sha256RSA</td>
<td>16 December 2010</td>
<td>17 October 2032</td>
<td>53 80 2c e5 18 4b 1e c1 0b d6 26 2c d1 08 ef 88 86 dd 2c 0e</td>
<td>db 18 ac 54 e8 d1 6c 01 93 dd 95 4e 18 53 7b 8a 71 b2 34 e7</td>
<td>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</td>
</tr>
</tbody>
</table>