Building a better
working world

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

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

Independent Assurance Report

To the management of Inera AB:

Scope

We have been engaged by Inera AB (Inera), in a reasonable assurance engagement, to report on the statements by the managements of Inera and Telia Company AB (Telia), an independent service organization that provides Certification Authority (CA) hosting services for Inera, that, except for matters described in the statements, for Inera's Certification Authority (CA) operations known as SITHS CA in Sweden and Finland, throughout the period 1 April 2017 through 31 March 2018 for Inera's CAs as enumerated in Attachment A, Inera and Telia have:

- disclosed their SSL certificate life cycle management business practices in their:
  - SITHS Certificate Policy v 1.2; and
  - TeliaSonera SITHS CA v1 CPS v1.2

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

And, for its CAs as enumerated in Attachment A

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

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

Certification Authority's responsibilities

Inera's and Telia's managements are responsible for their statements, including the fairness of their presentation, and the provision of their described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2.

Our independence and quality control

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

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

Auditor's responsibilities

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

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

(2) selectively testing transactions executed in accordance with disclosed SSL certificate life cycle management practices;

(3) testing and evaluating the operating effectiveness of the controls; and

(4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at Inera and 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, Inera's and Telia's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Basis for qualified opinion

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

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

#	Deviation	Relevant WebTrust Criteria
1	The CA has not disclosed in its Certificate Policy (CP) or Certification Practices Statement (CPS) that it does not review CAA (Certification Authority Authorisation) DNS Records. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 1, Criterion 6 to not be met.	**Principle 1, Criterion 6** The CA discloses in its Certificate Policy (CP) and/or Certification Practices Statement (CPS) under section 4.2 (if the CA's disclosures follow RFC 3647) or under section 4.1 (if the CA's disclosures follow RFC 2527) whether the CA reviews CAA (Certification Authority Authorisation) DNS Records, and if so, the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names. The CA maintains controls to provide reasonable assurance that it logs all actions taken, if any, consistent with its processing practice.
2	SSL certificates issued by the CA in the beginning of the reporting period from 1 April 2017 to 19 April 2017 did not contain subject:localityName or subject:stateOrProvinceName field. Subject:localityName field was included in the certificates from 20 April 2017 onwards. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 2, Criterion 2.14 to not be met.	**Principle 2, Criterion 2.14** The CA maintains controls to provide reasonable assurance that Subject information of Certificates conforms to the Baseline Requirements, including: … • subject:localityName • subject:stateOrProvinceName …
3	The security configurations of all the relevant systems had not been reviewed on at least a weekly basis. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 4, Criterion 1.8 to not be met.	**Principle 4, Criterion 1.8** The CA maintains controls to provide reasonable assurance that configurations of Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are reviewed on at least a weekly basis to determine whether any changes violated the CA's security policies.
4	Human review of logs had not covered all the relevant application and system logs and that some log reviews had not always been performed at least every 30 days. In addition testing that the monitoring, logging, alerting, and log-integrity-verification functions were operating properly had not been performed during the reporting period. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 4, Criterion 3.5 to not be met.	**Principle 4, Criterion 3.5** The CA maintains controls to provide reasonable assurance that a human review of application and system logs is performed at least every 30 days and includes: • Validating the integrity of logging processes; and • Testing the monitoring, logging, alerting, and log-integrity-verification functions are operating properly.
5	The CA had not documented its vulnerability correction process. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 4, Criterion 4.2 to not be met.	**Principle 4, Criterion 4.2** The CA maintains controls to provide reasonable assurance that a formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities.

Qualified Opinion

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

- disclosed their SSL certificate life cycle management business practices in their:
  - SITHS Certificate Policy v 1.2; and
  - TeliaSonera SITHS CA v1 CPS v1.2

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

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

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

Copenhagen June 29, 2018

Ernst & Young P/S
Godkendt Revisionspartnerselskab

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

Juha Sunila
Senior Manager, CISA, CISSP

Attachment A: List of CAs in Scope

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

CA #	Cert. #	Subject	Issuer	Serial	Key Algorithm and Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA1 Fingerprint
1	1	CN = SITHS Root CA v1 O = Inera AB C = SE	self-signed	00 90 66 61 a8 62 3d 65 44 77 04 3f 71 9a c3 97 0c	RSA 4096 bits	sha1RSA	29 March 2012	29 March 2032	32 f9 9d 4f 69 e9 98 8d a0 d6 8c 7d f9 1d ce a3 3c ba 76 15	58 5f 78 75 be e7 43 3e b0 79 ea ab 7d 05 bb 0f 7a f2 bc cc
3	1	CN = SITHS Type 3 CA v1 O = Inera AB C = SE	SITHS Root CA v1	00 90 95 43 ba 0d 26 4a 02 c7 31 0b 6a f9 67 af 0c	RSA 4096 bits	sha512RSA	8 May 2012	8 May 2022	2b c2 66 ca fc 48 7c 2f 24 1d 85 3b 9a 70 6c af 29 4a c9 05	b6 54 72 a5 9c 02 4a 57 5f bc 48 9d 4a 33 05 96 32 e6 9d aa

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

CA #	Cert. #	Subject	Issuer	Serial	Key Algorithm and Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA1 Fingerprint
2	1	CN = SITHS Type 1 CA v1 O = Inera AB C = SE	SITHS Root CA v1	00 ce b8 10 45 13 f4 24 13 6c 36 03 89 6e a6 f4 12	RSA 4096 bits	sha1RSA	8 May 2012	8 May 2022	95 9d 7c 35 4d ed fd d2 ba 3f 5f bd 8a 85 f2 3c 5b 26 3f f4	90 57 eb ee c9 f3 5d ce 8e ae fd 9e 03 88 10 69 79 8a 67 7d

inera

Inera's Management Statement

Inera AB (Inera) operates the Certification Authority (CA) services known as SITHS CA as enumerated in Attachment A, and provides SSL CA services.
Inera management has assessed its disclosure of its certificate practices and controls over its SSL CA services. During our assessment we noted the following deviations which caused the relevant criteria to not be met:

#	Deviation	Relevant WebTrust Criteria
1	The CA has not disclosed in its Certificate Policy (CP) or Certification Practices Statement (CPS) that it does not review CAA (Certification Authority Authorisation) DNS Records. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 1, Criterion 6 to not be met.	**Principle 1, Criterion 6** The CA discloses in its Certificate Policy (CP) and/or Certification Practices Statement (CPS) under section 4.2 (if the CA's disclosures follow RFC 3647) or under section 4.1 (if the CA's disclosures follow RFC 2527) whether the CA reviews CAA (Certification Authority Authorisation) DNS Records, and if so, the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names. The CA maintains controls to provide reasonable assurance that it logs all actions taken, if any, consistent with its processing practice.
2	SSL certificates issued by the CA in the beginning of the reporting period from 1 April 2017 to 19 April 2017 did not contain subject:localityName or subject:stateOrProvinceName field. Subject:localityName field was included in the certificates from 20 April 2017 onwards. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 2, Criterion 2.14 to not be met.	**Principle 2, Criterion 2.14** The CA maintains controls to provide reasonable assurance that Subject information of Certificates conforms to the Baseline Requirements, including: ... • subject:localityName • subject:stateOrProvinceName ...

Based on that assessment, in Inera management's opinion, except for the matters described in the preceding table, in providing its Certification Authority (CA) services in Sweden, throughout the period 1 April 2017 to 31 March 31 2018, Inera has:

- disclosed its SSL certificate life cycle management business practices in its
  - SITHS Certificate Policy v 1.2

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Inera website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that
  - the integrity of keys and SSL certificates it manages is established and protected throughout their life cycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by Inera)
- maintained effective controls to provide reasonable assurance that

inera

- logical access to CA systems and data is restricted to authorized individuals;
- the continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

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

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

Inera has outsourced hosting of its CA services to Telia. Our statement does not extend to controls exercised by Telia.

Stockholm, 29 June 2018

Petter Könberg
Head of Department
Inera AB

Attachment A: List of CAs in Scope

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

CA #	Cert. #	Subject	Issuer	Serial	Key Algorithm and Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA1 Fingerprint
1	1	CN = SITHS Root CA v1 O = Inera AB C = SE	self-signed	00 90 66 61 a8 62 3d 65 44 77 04 3f 71 9a c3 97 0c	RSA 4096 bits	sha1RSA	29 March 2012	29 March 2032	32 f9 9d 4f 69 e9 98 8d a0 d6 8c 7d f9 1d ce a3 3c ba 76 15	58 5f 78 75 be e7 43 3e b0 79 ea ab 7d 05 bb 0f 7a f2 bc cc
3	1	CN = SITHS Type 3 CA v1 O = Inera AB C = SE	SITHS Root CA v1	00 90 95 43 ba 0d 26 4a 02 c7 31 0b 6a f9 67 af 0c	RSA 4096 bits	sha512RSA	8 May 2012	8 May 2022	2b c2 66 ca fc 48 7c 2f 24 1d 85 3b 9a 70 6c af 29 4a c9 05	b6 54 72 a5 9c 02 4a 57 5f bc 48 9d 4a 33 05 96 32 e6 9d aa

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

CA #	Cert. #	Subject	Issuer	Serial	Key Algorithm and Size	Digest Algorithm	Not Before	Not After	Subject Key Identifier	SHA1 Fingerprint
2	1	CN = SITHS Type 1 CA v1 O = Inera AB C = SE	SITHS Root CA v1	00 ce b8 10 45 13 f4 24 13 6c 36 03 89 6e a6 f4 12	RSA 4096 bits	sha1RSA	8 May 2012	8 May 2022	95 9d 7c 35 4d ed fd d2 ba 3f 5f bd 8a 85 f2 3c 5b 26 3f f4	90 57 eb ee c9 f3 5d ce 8e ae fd 9e 03 88 10 69 79 8a 67 7d

TELIA'S MANAGEMENT STATEMENT

Telia Company AB (Telia), an independent service organization (subservice organization), provides Certification Authority (CA) hosting services to Inera AB (Inera) for Inera's SSL CA services known as SITHS CA.

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

#	Deviation	Relevant WebTrust Criteria
1	The security configurations of all the relevant systems had not been reviewed on at least a weekly basis. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 4, Criterion 1.8 to not be met.	**Principle 4, Criterion 1.8** The CA maintains controls to provide reasonable assurance that configurations of Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are reviewed on at least a weekly basis to determine whether any changes violated the CA's security policies.
2	Human review of logs had not covered all the relevant application and system logs and that some log reviews had not always been performed at least every 30 days. In addition, testing that the monitoring, logging, alerting, and log-integrity-verification functions were operating properly had not been performed during the reporting period. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 4, Criterion 3.5 to not be met.	**Principle 4, Criterion 3.5** The CA maintains controls to provide reasonable assurance that a human review of application and system logs is performed at least every 30 days and includes: • Validating the integrity of logging processes; and Testing the monitoring, logging, alerting, and log-integrity-verification functions are operating properly.
3	The CA had not documented its vulnerability correction process. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, Principle 4, Criterion 4.2 to not be met.	**Principle 4, Criterion 4.2** The CA maintains controls to provide reasonable assurance that a formal documented vulnerability correction process is followed and includes identification, review, response, and remediation of vulnerabilities.

Based on that assessment, in Telia management's opinion, except for the matters described in the preceding table, in providing its Certification Authority (CA) services in Sweden and Finland, throughout the period 1 April 2017 to 31 March 31 2018, Telia has:

- disclosed its SSL certificate lifecycle management business practices in its
  - TeliaSonera SITHS CA v1 CPS v1.2

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

- CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

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

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

Telia provides CA hosting services to Inera as an independent service organization. Our statement does not extend to controls exercised by Inera.

Stockholm, 29 June 2018

Telia Company AB

Shahryar Khan
Head of GSO NW Transport Automation and Systems