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 Inera's statement, 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 business, key life cycle management, certificate life cycle management, and CA environmental control practices in their:
  - SITHS Certificate Policy v 1.2; and
  - TeliaSonera SITHS CA v1 CPS v1.2
- maintained effective controls to provide reasonable assurance that
  - Telia's Certification Practice Statement is consistent with Inera's Certificate Policy; and
  - Inera provides its services in accordance with its Certificate Policy and 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 they manage is established and protected throughout their life cycles;
  - the integrity of subscriber keys and certificates they manage is established and protected throughout their life cycles;
  - subscriber information is properly authenticated (for the registration activities performed by Inera and 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 Trust Services Principles and Criteria for Certification Authorities v.2.0.

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

Inera does not escrow its CA keys and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.

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 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 Inera's and Telia's key and certificate life cycle management business practices and their 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 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.

[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:

#	Deviation	Relevant WebTrust Criteria
1	As part of the implementation of the new Swedish public sector PKI platform Efos, private keys of SITHS Root CA v1 and its subordinate CAs were copied and private key copies transported on 21 March 2018 from Telia that is hosting Inera's current CA systems to Försäkringskassan that will host the new Efos platform. We were unable to test and determine whether Försäkringskassan maintained controls to provide reasonable assurance that the CA private key copies hosted by them remain confidential and maintain their integrity and that the CA's private keys are backed up, stored and recovered by authorized personnel in trusted roles, using multiple person control in a physically secured environment throughout the period 21 March 2018 to 31 March 2018. This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 4.2 to not be met.	**4.2 CA Key Storage, Backup and Recovery** The CA maintains controls to provide reasonable assurance that CA private keys remain confidential and maintain their integrity. The CA's private keys are backed up, stored and recovered by authorized personnel in trusted roles, using multiple person control in a physically secured environment.

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 business, key life cycle management, certificate life cycle management, and CA environmental control practices in their:
  - SITHS Certificate Policy v 1.2; and
  - TeliaSonera SITHS CA v1 CPS v1.2
- maintained effective controls to provide reasonable assurance that
  - Telia's Certification Practice Statement is consistent with Inera's Certificate Policy; and
  - Inera provides its services in accordance with its Certificate Policy and 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 they manage is established and protected throughout their life cycles;
  - the integrity of subscriber keys and certificates they manage is established and protected throughout their life cycles;
  - subscriber information is properly authenticated (for the registration activities performed by Inera and 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 Services Principles and Criteria for Certification Authorities v.2.0.

This report does not include any representation as to the quality of Inera's and Telia's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.0, 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

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
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
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

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 the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management
- Integrated circuit card life cycle management
- Subordinate CA certification

The management of Inera 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 Inera's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.
Inera management has assessed its disclosure 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:

#	Deviation	Relevant WebTrust Criteria
1	As part of the implementation of the new Swedish public sector PKI platform Efos, private keys of SITHS Root CA v1 and its subordinate CAs were copied and private key copies transported on 21 March 2018 from Telia that is hosting Inera's current CA systems to Försäkringskassan that will host the new Efos platform. The management was unable to assess whether Försäkringskassan maintained controls to provide reasonable assurance that the CA private key copies hosted by them remain confidential and maintain their integrity and that the CA's private keys are backed up, stored and recovered by authorized personnel in trusted roles, using multiple person control in a physically secured environment throughout the period 21 March 2018 to 31 March 2018. This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 4.2 to not be met.	**4.2 CA Key Storage, Backup and Recovery** The CA maintains controls to provide reasonable assurance that CA private keys remain confidential and maintain their integrity. The CA's private keys are backed up, stored and recovered by authorized personnel in trusted roles, using multiple person control in a physically secured environment.

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:

inera

- disclosed its business, key life cycle management, certificate life cycle management, and CA environmental control practices in its
  - SITHS Certificate Policy v 1.2
- maintained effective controls to provide reasonable assurance that
  - Telia's Certification Practice Statement was consistent with Inera's Certificate Policy; and
  - Inera provided its services in accordance with its Certificate Policy
- 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 Inera); and
  - subordinate CA certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that
  - 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

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

CA Business Practices Disclosure

- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- System Access Management
- Systems Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

inera

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
- Integrated Circuit Card (ICC) Life Cycle Management
- 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

Inera has outsourced hosting of its CA services to Telia. Inera is responsible for its Certificate Policy and Telia for its Certificate Practice Statement. Inera does not have its own Certificate Practice Statement document, does not escrow its CA keys, and does not provide certificate suspension services. Accordingly, our statement does not extend to controls that would address those criteria and it 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

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
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
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

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 CA services known as SITHS CA.

The management of Telia is responsible for establishing and maintaining effective controls over its CA hosting services for Inera, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle 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 provide only 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 for Inera. Based on that assessment, in Telia management's opinion, in providing its Certification Authority (CA) hosting services for Inera in Sweden and Finland, 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
  - TeliaSonera SITHS CA v1 CPS v1.2
- maintained effective controls to provide reasonable assurance that:
  - Telia provides its services in accordance with its Certification Practice Statement
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - the integrity of subscriber keys and certificates it manages was 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
- Integrated Circuit Card (ICC) Life Cycle Management
- Requirements for Subscriber Key Management

Certificate Life Cycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

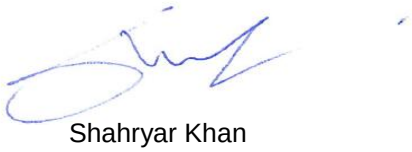
Subordinate CA Certificate Life Cycle Management Controls

- Subordinate CA Certificate Life Cycle Management

Telia provides CA hosting services to Inera as an independent service organization. Telia is not responsible for Certificate Policy document, does not escrow CA keys, and does not provide certificate suspension services. Accordingly, our statement does not extend to controls that would address those criteria and it 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