**General information about the CA’s associated organization**

CA Company Name: Inera AB

Website URL: www.inera.se

Organizational type: Corporation established by the government

Primary Market / Customer Base: Swedish healtchare organizations, public and private

Impact to Mozilla Users Describe the types of Mozilla users who are likely to encounter your root certificate as relying parties Users who come into contact with swedish healthcare

CA Contact Information: sithspolicyauthority@inera.se

**Technical information about each root certificate**

Certificate Name: SITHS Root CA v1

Certificate Issuer Field: CN = SITHS Root CA v1

O = Inera AB

C = SE

Certificate Summary: This root CA issues certificate to subordinate issuing CAs. Subordinate issuing CAs issue certificates for persons and functions (e.g. applications, servers etc.)

Root Cert URL: http://aia.siths.se/sithsrootcav1.cer

SHA1 Fingerprint: 58 5f 78 75 be e7 43 3e b0 79 ea ab 7d 05 bb 0f 7a f2 bc cc

Valid From: 2012-03-29

Valid To: 2032-03-29

Certificate Version 1

Certificate Signature Algorithm sha1RSA

Signing key parameters RSA modulus length: RSA 4096

Test Website URL (SSL) https://v1.test.msoft.siths.se

CRL URL: http://crl1.siths.se/sithsrootcav1.crl

NextUpdate for CRLs of end-entity certs: 48 hours

Test:

OCSP URL OCSP URI in the AIA of end-entity: http://ocsp1.siths.se

Testing results

a) Browsing to test website with OCSP enforced in Firefox browser

b) If requesting EV: https://wiki.mozilla.org/PSM:EV\_Testing\_Easy\_Version

SSL Validation Type: Domain validation

**CA Hierarchy information for each root certificate**

CA Hierarchy List, description, and/or diagram of all intermediate CAs signed by this root.



**Verification Policies and Practices**

Policy Documentation Language(s) that the documents are in:

CP: English

CPS: English

Relying Party Agreement: English

Audits Audit Type: Webtrust Audit for Certification Authorities

Auditor: Ernst & Young

Auditor Website: http://www.ey.com/

Multi-factor Authentication: Required for all RAs and CA-personell

Network Security: Applied accordin to requirements