**Bugzilla ID: 792337**

**Buzilla Summary: Add SITHS Root CA Cert to Root CA Store**

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

CA Company Name: Inera AB

Website URL: http://www.inera.se/infrastrukturtjanster/SITHS

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>

Regarding the OCSP-error that you encountered, this is caused by the fact that Firefox does not handle certficates that have more than one OCSP-path specified within certificates (it only tries the last path specified within a certficate). Since the last path specified within SITHS certificates points to an isolated network it will not work, however the primary path does point to an Internet location (http://ocsp1.siths.se).

I have reported this as a bug with Bugzilla ID 797815.

CRL URL: http://crl1.siths.se/sithstype2cav1.crl and http://crl2.siths.sjunet.org/sithstype2cav1.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> and <http://ocsp2.siths.sjunet.org>

Requested Trust Bits: Websites (SSL/TLS)

 Email (S/MIME)

 Code Signing

SSL Validation Type: DV

EV Policy OID(s) Not applicable, not requesting EV treatment.

**CA Hierarchy information for each root certificate**

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



Externally Operated subCAs: All subCAs are centrally operated and covered by the SITHS Certificate policy and Certificate Practice Statements.

Cross-Signing: Not used by SITHS.

Technical Constraints on Third-party Issuers: See the SITHS Certificate Policy.

**Verification Policies and Practices**

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

CP: English <http://www.inera.se/Documents/Infrastrukturtjanster/Identifieringstjanst_SITHS/Anslutningsdokument_Inera/SITHS-certifikat/siths_certicate_policy.pdf>

CPS: English

<http://www.inera.se/Documents/Infrastrukturtjanster/Identifieringstjanst_SITHS/Anslutningsdokument_Inera/SITHS-certifikat/telia_sonera_siths_ca_v1_cps_version_1.0.pdf>

Relying Party Agreement: English

<http://www.inera.se/Documents/Infrastrukturtjanster/Identifieringstjanst_SITHS/Anslutningsdokument_Inera/SITHS-certifikat/siths_relying_party_agreement.pdf>

Audits Audit Type: Webtrust Audit for Certification Authorities <https://cert.webtrust.org/ViewSeal?id=1383>

Auditor: Ernst & Young

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

Baseline Requirements (SSL): Fully compliant with the CAB Forum baseline requirements.

SSL Verification Procedures: See the SITHS Certificate Policy.

Organization verification Procedures: See the SITHS Certificate Policy.

Email Address Verification Procedures: See the SITHS Certificate Policy.

Code Signing Subscriber
Verification Procedures: See the SITHS Certificate Policy.

Multi-factor Authentication: See the SITHS Certificate Policy.

Network Security: See the SITHS Certificate Policy.