Bugzilla ID: 792337
Bugzilla Summary: Add SITHS Root CA Cert to Root CA store

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

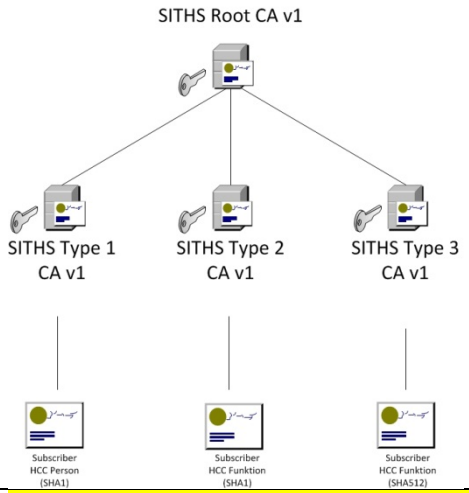
CA Company Name	Inera AB
Website URL	http://www.inera.se/Infrastrukturtjanster/SITHS
Organizational type	Corporation established by the government
Primark Market / Customer Base	SITHS certificates and e-ID's are issued to organizations/employees working within or having a business connection to the healthcare sector. The business connection should be delivering healthcare service. The potential number of users that access health care servers/services is the whole Swedish population, which exceeds 9 million people.
CA Contact Information	CA Email Alias: sithspolicyauthority@inera.se CA Phone Number: 08-452 72 72 Title / Department: SITH National Security Solution

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	SITHS is an abbreviation for Secure IT within Health care. 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	3
Certificate Signature Algorithm	SHA-1 RSA
Modulus	4096
Test Website URL (SSL)	https://v1.test.msoft.siths.se I imported the root cert into my FF browser, and tried to browse to this site, and I get: Error code: sec_error_ocsp_server_error Please test with OCSP enforced as described here https://wiki.mozilla.org/CA:Recommended_Practices#OCSP

	My guess is that the server is not sending the intermediate cert along with its SSL cert. Only root certs are included in Mozilla's root store.
CRL URL	http://crl1.siths.se/sithsrootcav1.crl NextUpdate for CRLs of end-entity certs: 48 hours
OCSP URL	http://ocsp1.siths.se
Requested Trust Bits	Which trust bits are you requesting for this root? One or more of: 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	
Externally Operated SubCAs	If this root has subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist
Cross-Signing	List all other root certificates for which this root certificate has issued cross-signing certificates. List all other root certificates that have issued cross-signing certificates for this root certificate. If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.
Technical Constraints on Third-party Issuers	Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate

Verification Policies and Practices

Policy Documentation	Document Repository: http://www.inera.se/SITHSDokument CP: (please provide direct link, to English version preferred) CPS: (please provide direct link, to English version preferred) Relying Party Agreement:
Audits	Audit Type: WebTrust Auditor: Ernst & Young, http://www.ey.com Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=1216 (2011.03.31) Please provide audit statement for this year.
Baseline Requirements (SSL)	What is your status in regards to complying with the CAB Forum Baseline Requirements? (https://www.cabforum.org/Baseline_Requirements_V1.pdf)
SSL Verification Procedures	If you are requesting to enable the Websites Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Organization Verification Procedures	
Email Address Verification Procedures	If you are requesting to enable the Email Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Code Signing Subscriber Verification Procedures	If you are requesting to enable the Code Signing Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Multi-factor Authentication	Please provide document (CP/CPS) section where this is defined.
Network Security	Please provide document (CP/CPS) section where this is defined.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	
CA Hierarchy	
Audit Criteria	
Document Handling of IDNs in CP/CPS	
Revocation of Compromised Certificates	
Verifying Domain Name Ownership	
Verifying Email Address Control	
Verifying Identity of Code Signing Certificate Subscriber	
DNS names go in SAN	
Domain owned by a Natural Person	
OCSP	

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	

Wildcard DV SSL certificates	
Email Address Prefixes for DV Certs	If DV SSL certs, then list the acceptable email addresses that are used for verification.
Delegation of Domain / Email validation to third parties	
Issuing end entity certificates directly from roots	
Allowing external entities to operate subordinate CAs	
Distributing generated private keys in PKCS#12 files	
Certificates referencing hostnames or private IP addresses	
Issuing SSL Certificates for Internal Domains	
OCSP Responses signed by a certificate under a different root	
CRL with critical CIDP Extension	
Generic names for CAs	
Lack of Communication With End Users	