Bugzilla ID: 544362
Bugzilla Summary: Add SITHS_CA_v3 root certificate

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Info	Data
CA Name	Inera AB
Website URL	http://www.inera.se/Infrastrukturtjanster/SITHS/
Organizational type	Swedish healthcare organization. Inera AB is not a private company. Inera AB is sponsored by the twenty Swedish county councils.
Primary 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: kundstod@inera.se CA Phone Number: 08-452 72 72, Title / Department: SITH National Security Solution

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data
Certificate Name	SITHS CA v3 Note: O is Carelink due to a company merge
	SITHS is an abbreviation for Secure IT within Health care. The name of the company has been changed from Sjukvårdsrådgivningen (translates to Health Care Guidance) to Inera AB. The organization working with SITHS remains the same. The name SITHS was originally owned by Carelink AB. Carelink was sponsored in a similar way as Sjukvårdsrådgivningen. The two companies were merged two and a half years ago.
Cert summary / comments	The purpose of this root is to enable confidentiality, integrity, authenticity and non-repudiation when exchanging information between the different actors within the Swedish healthcare sector. SITHS certificates are also used to secure the exchange of healthcare related information between the healthcare sector and government agencies. SITHS certificates and e-ID's are only issued to organizations/employees working within or having a business connection to the healthcare sector. SITHS certificates are not issued to the receiver of healthcare services (patients).
The root CA certificate URL	http://www.inera.se/VirtDocRoot%5CTj%C3%A4nster%5CSITHS%5CVisas%20p%C3%A5%20bolagswebb/09.%20Rotcertifikat/SITHS_CA_v3.cer

SHA-1 fingerprint	16:D8:66:35:AF:13:41:CD:34:79:94:45:EB:60:3E:27:37:02:96:5D
Valid from	2005-11-28
Valid to	2015-11-28
Cert Version	3
Modulus length	2048
Test Website	https://test.siths.se/
CRL URL	CRL URL: http://www.carelink.se/siths-ca/ca003.crl (NextUpdate: 1 day) CRL Distribution Point: URI: ldap://sithscrl.carelink.sjunet.org/cn=SITHS%20CA%20ver%203,o=SITHS%20CA,c=SE?certificateRevocationList;binary?
OCSP Responder URL	http://sithsocsp.trust.telia.com >> Test Website: https://test.siths.se/ When I browse to the test website in my Firefox browser with OCSP enforced, I get the error sec_error_ocsp_server_error. Please see https://wiki.mozilla.org/CA:Recommended_Practices#OCSP for how to enforce OCSP in your Firefox browser for testing. Note that I am able to browse to the test website when I don't have OCSP enforced.
CA Hierarchy	There are no subordinate CAs. The root is protected using Hardware Secure Module in a medium meeting FIPS 140-2 Level 3.
Sub-CAs operated by 3rd parties	None
Cross-Signing	None
Requested Trust Bits	Websites Email
SSL Validation Type DV, OV, and/or EV	OV Comment #7: We perform both organization and domain verifications for all customers. The only exception to this routine is if a recently checked organization orders one more certificate with a cn consisting of a domain name we already have written confirmation that they own.
EV policy OID(s)	Not requesting EV-enablement
CP/CPS	SITHS document repository: http://www.inera.se/Infrastrukturtjanster/SITHS/Dokument-for-SITHS/ SITHS Routine Verification of Organizations and Representatives (Swedish): http://www.inera.se/VirtDocRoot%5CTj%C3%A4nster%5CSITHS%5CVisas%20p%C3%A5%20bolagswebb/03.%20Styrande%20dokument/SITHS%20rutin%20f%C3%B6r%20verifiering%20av%20organisationer%20och%20ombud%20ver%202.0.pdf Target audience of this document is CA and RA personnel SITHS CA. The purpose of this document is to describe how the certificate information is verified and the order accuracy ensured. This document specifies how SITHS CA ensures a proper validation of the applying organization, the ownership of the domain name and the certificate request. This document is based on http://cabforum.org/EV_Certificate_Guidelines.pdf and adapted for local regulations within the Swedish healthcare sector.

	Certificates for Swedish Health and Social Care (HCC) (Swedish): http://www.inera.se/VirtDocRoot%5CTj%C3%A4nster%5CSITHS%5CVisas%20p%C3%A5%20bolagswebb/03.%20Styrande%20dokument/HCC%20Version%202%2035.pdf SITHS Certificate Policy (Swedish): http://www.inera.se/VirtDocRoot%5CTj%C3%A4nster%5CSITHS%5CVisas%20p%C3%A5%20bolagswebb/02.%20Styrande%20dokument/SE-SITHS-CA-Policy-4.pdf This certificate policy describes the procedures and practices for issuing certificates for individuals, organizations and functions in health and social care in Sweden, called Healthcare Certificates (HCC). Description of procedures and organizations for the purposes of this certificate policy must be provided in a separate so-called Certification Practice Statement (CPS), published by the CA to apply this policy. If the CA applying this policy, choose to tie a Registration Authority (RA) for the identification of key holders and the collection of properties of key holder, this RA work under the RA policy and published by RA Registration Authority Practice Statement (RAPS) that describes procedures and structures for the implementation of RA policy. SITHS Registration Authority Policy (Swedish): http://www.inera.se/VirtDocRoot%5CTj%C3%A4nster%5CSITHS%5CVisas%20p%C3%A5%20bolagswebb/02.%20Styrande%20dokument/SE-SITHS-RA-Policy-4.pdf Telia Certification Practice Statement for certificates issued according to the SITHS CA Policy (Swedish): http://www.inera.se/VirtDocRoot%5CTj%C3%A4nster%5CSITHS%5CVisas%20p%C3%A5%20bolagswebb/02.%20Styrande%20dokument/Telia_SITHS_CPS_v2.0.pdf This document contains Telia CPS for issuing certificates for HCC in Sweden. SITHS CA-policy version 3A 2006-02-01 has been the basis for the development of the original version of this CPS. Audit of CPS: one has subsequently been made in connection with the re-vision of the SITHS CA policy. CPS: one assumes that local RA (Registration Authority), and the RA to perform its obligations which describes how the RA meets the regulatory framework of the SITHS RA policy. This document is owned by TeliaSonera Sweden AB and managed by TeliaSonera and TeliaSonera singled out by the organization.
AUDIT	Audit Type: WebTrust CA Auditor: Ernst & Young Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=991 (2009.06.30)
Organization Verification	Comment #3: Functional/organizational certificate (soft certificate) The company is checked using the service of the Swedish companies registration office (www.bolagsverket.se) to ensure that: · the company exists · the business is healthcare related · the person signing the service agreement with Sjukvårdsrådgivningen is a member of the board

	SITHS Routine Verification of Organizations and Representatives (Swedish): http://www.inera.se/VirtDocRoot%5CTj%C3%A4nster%5CSITHS%5CVisas%20p%C3%A5%20bolagswebb/03.%20Styrande%20dokument/SITHS%20rutin%20f%C3%B6r%20verifiering%20av%20organisationer%20och%20ombud%20ver%202.0.pdf Google Translations: Section 2: SITHS CA verifies the RA organization requesting information through independent and constantly updated data sources. SITHCS CA uses the following data sources to verify the domain and company information: Domain Control: www.iis.se, domaininfo.com, www.nunames.nu/udrp.htm, ipkoll.se/natverkstjanster/whois, www.ripe.net Company Information: www.bolagsverket.se, www.ratsit.se Section 2.1. Legal existence and identity SITHS CA shall verify, through the application named the organization's legislative body, to applicant company, the certificate of request time, is a valid and existing companies in the named organization / domain authority and the organization's legal name in Certificate application complies with the named organization official name. 2.1.1. Verification of organizations Within the public sector, a public organization to be established under the political leadership, example, a county have a County Council. In private business, the organization must be legally valid and active. Regardless of ownership the organization must demonstrate a verifiable and physical existing business. At least one natural person as belonging to the applicant organization and the right to sign the name must be identifiable and verifiable. This person must be either self-sign the service contract or by proxy give another person the right to sign service contracts with Inera AB. • Verification should be carried out through independent sources, see Section 2. • Certificates may be issued only to active organizations operating in Sweden. • Verify the applicant organization designated organization's name and corporate identity with the authority, organization or "Registration Office" (the source reference for the Corporate Data); who have accurate information about the applicant organization. • Verify that the requesting organization's name is correct and that it is consistent with a Name of organization uses in public. • Verify that the applicant organization exists legally, is active (ie not being suspended, declared in bankruptcy or similar) and that the activities of the requesting organization stated that it is consistent with the information about the activities held by "Registration Office". • Obtain from the "Registration Office" the organization's physical address or organization representatives, only the mailbox and post office box is not enough. • Verify that the URL actually is the correct address and that it is the address given in Certificate application. If in doubt:

	identifying the organization's buildings, and though it seems a permanent building. Identify the signs of organization appears to be permanent or only temporary. Identify if there are signs that the organization actually engage activities or not. Identify surrounding environment, such as street names or photographs in which similar can be identified. 2.1.2. Verification of the organization's representatives The identity of the organization's representative must be verified directly physically or via a "Registration Agency". If the identity verified through a "Registration agency" may be governed by the information made available over the Internet, taking direct contact as well as letters, e-mail or telephone correspondence. Contact is verified by an independent source reference, see Section 2. • The organization's representatives identified in a physical meeting, or by direct contact via telephone, e-mail or letter. Ineras CA could also rely on a previously completed the identification. • The organization's representative at the meeting physically prove their identity with authentic identification document (Swedish driving license, Swedish passport, ID document SIS approved, national identity cards, Tax ID card or an approved e-ID). • Verification of the right to represent the applicant organization may be made by telephone request, callback, letter or e-mail by CA to the organization's representatives, its administrative activities or through legal documents. • Checks to be carried out to verify that the given phone number goes to the requesting organization's contact person, phone number to see the organization's official telephone records, that phone number, if there is one mobile phone number, contact person is not the main telephone connection. In the control at the initial registration, including dialing by the organization's official telephone implemented to ensure that at least two independent phone tested. • Verification that the representative / client work for connecting the organization shall be made through independent sources. • The certification order, the customer must specify who is authorized recipients of the issued Certificate. Before issuing the customer must confirm that the certificate request sent. Feedback from CA can be oral or written. Section 2.3: SITHS CA shall take the necessary steps to verify that, at the time the certificate is issued, owner of the certificate mentioned in the application has given full powers on the requesting party to use the certificate (Certificates). If the owner is one of the other party requesting the certificate is a formalized permission or consent documented. Certificate Requests must be made by qualified buyers. Examples of qualified buyers is a representative the requesting organization (directly or as an agent) or a representative of a third party who delivers a service to another organization. These characteristics also apply for approval of certificate request and contract signatures. • A valid contract must exist, see Section 2.5 • The organization and the organization's representative, shall be verified, see Section 2.1 • The right to use of the domain must be proved, see section 2.2 2.4. The correctness of the certificate's details SITHS CA shall take the necessary steps to verify that, at the time the certificate is issued, all other information in the certificate application is correct. Certificate Request must be complete (cf. "Service Agreement Annex SITHS Order" or equivalent) and the data that it shall at least include: • Client's organization name

	• Client's corporate identity • Client's request for a domain and DNS names for certificates • Order entry and billing addresses • Order appropriate contractual signatories and their contact details • Client competent customer and recipient and their contact details
Domain Name Ownership / Control	SITHS Routine Verification of Organizations and Representatives (Swedish): http://www.inera.se/VirtDocRoot%5CTj%C3%A4nster%5CSITHS%5CVisas%20p%C3%A5%20bolagswebb/03.%20Styrande%20dokument/SITHS%20rutin%20f%C3%B6r%20verifiering%20av%20organisationer%20och%20ombud%20ver%202.0.pdf Google Translations: Section 2: SITHS CA verifies the RA organization requesting information through independent and constantly updated data sources. SITHS CA uses the following data sources to verify the domain and company information: Domain Control: www.iis.se, domaininfo.com, www.nunames.nu/udrp.htm, ipkoll.se/natverkstjanster/whois, www.ripe.net Company Information: www.bolagsverket.se, www.ratsit.se 2.2. The right to the domain SITHS CA shall take the necessary steps to verify that, at the time of certificate issuance, the organization requesting the certificate has the unique right to use the domain name (domain names) in application that will be used in certificates. The verification of domain ownership takes place through the WHOIS search with the Foundation for Internetinfrastrukturs (IIS) web service. If the requesting organization is not the owner of the certificate in the name input domain name authenticated access rights via mail, e mail, telephone or domain owner faxkorrespondens with. Domain owner contacted by using the WHOIS contact information given in response to the question, see Section 2. • The domain name will be based on a registered company name and behave in agreement with the Internet Corporation for Assigned Names and Numbers (ICANN) and Internet Assigned Numbers Authority (IANA) (reference source for Domain Controllers). • The organization shall be the owner of the domain name or the domain owner have been given exclusive the right to use the certificate name. The proxy must be in the latter case be presented. Credentials are verified by domain owner. • If the domain owner can not be contacted, Inera CA allow the use of certificates in the name input domain name of the commissioning organization clearly and publicly identified themselves and that valid contract between the owner and the domain of the requesting organization exists. Inera CA publishes executed order on an agreed and controlled access point, such as secured Web page that requires account for reading / writing data.
Email Address Ownership / Control	Comment #7: The verification of that the certificate subscriber owns/controls the email address to be included in the certificate is only applicable for the issuing of electronic identities for employees and contractors. The procedure is described in the CA, RA and KRA policys. Comment #9: All certificates issued to persons are in the form of hard certificates on smart cards. Hard certificates in the form of

	electronic identity cards (SIS standard 614314) are only issued to employees and contractors. Only employees are allowed to get electronic identity cards with photo (valid for identification). A prerequisite for obtaining personal certificates is that the employing company has signed agreement with Inera AB. The agreement states that the company has to follow the policies mentioned above. The agreement also states that Inera AB are allowed to perform audits to ensure that the policies are followed.
Identity of Code Signing Subscriber	Note applicable. Not requesting the code signing trust bit.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  ○ SSL certs are OV.
	• Wildcard DV SSL certificates
	  ○ SSL certs are OV.
	• Email Address Prefixes for DV SSL Certs
	  ○ SSL certs are OV.
	• Delegation of Domain / Email validation to third parties
	  ○ Comment #7: **All county councils and a few major care takers have RA status (following our policies) which means that they administer their own domain/subdomain. According to the contract it is mandatory for them to follow our policies. We perform audits to ensure that the policies and routines are followed.**
	• Issuing end entity certificates directly from roots
	  ○ **End-entity certs are issued directly from the root. See above.**
	• Allowing external entities to operate unconstrained subordinate CAs
	  ○ Not applicable.
	• Distributing generated private keys in PKCS#12 files
	  ○ Comment #7: Not done.
	• Certificates referencing hostnames or private IP addresses
	  ○ Comment #7: DNS-name standard is used to ensure uniqueness server names. Certificates is not issued for private IP addresses.
	• Issuing SSL Certificates for Internal Domains
	  ○ Comment #7: Not done.
	• OCSP Responses signed by a certificate under a different root
	  ○ Comment #7: the OCSP response is signed by the same root.
	• CRL with critical CIDP Extension
	  ○ CRLs import into my Firefox browser without error.
	• Generic names for CAs
	  ○ CN has SITHS in it. O is Carelink due to a company merge