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 Information	Data
CA Name	Sjukvårdsrådgivningen SVR AB (SITHS)
Website URL (English version)	http://www.sjukvardsradgivningen.se http://www.carelink.se (companies merged)
Organizational type	Please specify the type of organization. e.g. is the CA operated by a private or public corporation, government agency, academic institution or consortium?
Primary market / customer base	Swedish healthcare sector The potential number of users that access health care servers/services is the whole Swedish population, which exceeds 9 million people. SITHS certificates and e-ID's are only issued to organizations/employees working within or having a business connection to the healthcare sector. The business connection should be delivering healthcare service. In other words, SITHS certificates are not issued to the receiver of healthcare services (patients).
CA Contact Information	CA Email Alias: An email alias is being requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization. CA Phone Number: A main phone number from which Mozilla can reach the organization responsible for root certificates for the CA. Title / Department: If Mozilla needed to call your main phone number, what Title/Department should the Mozilla representative ask for?

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
Cert summary / comments	
The root CA certificate URL	http://www.svrinfo.se/VirtDocRoot%5CTj%C3%A4nster%5CSITHS%5CVisas%20p%C3%A5%20bolagswebb/10.%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 / key length	2048
Test Website	For testing purposes, please provide a URL to a website whose SSL cert chains up to this root.
CRL URL	Please provide the URLs to the CRLs for this root and sub-CAs.
OCSP Responder URL	If you support OCSP, please provide the OCSP Responder URL.
CA Hierarchy	Please provide a list, description, and/or diagram of subordinate CAs under this root. Please indicate they types of certificates signed by each. Please indicate which sub-CAs are operated by the CA organization, and which are operated by external, third party organizations. For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CP/CPS, and that any audit covers them as well as the root.
Sub-CAs operated by 3rd parties	Does this root have any subordinate CAs that are operated by external third parties? For the subordinate CAs that are operated by third parties, please provide a general description and explain how the CP/CPS and audits ensure the third parties are in compliance. Also, see https://wiki.mozilla.org/CA:SubordinateCA_checklist If Mozilla accepts and includes the “SITHS CA v3 ” root, then we have to assume that we also accept any of your future sub-CAs and their sub-CAs. Therefore, the selection criteria for your sub-CAs and their sub-CAs will be a critical decision factor. Please point me to (and translate into English) the parts of the CP/CPS that clearly explain who can apply to operate a sub-CA (at any level), the selection/approval process for sub-CAs and their sub-CAs, the verification procedures applied to sub-CAs and their sub-CAs, what restrictions (legal and technical) are placed on all sub-CAs (eg constraints to issuing certs within certain domains).
Cross-Signing	Has this root be involved in cross-signing with any other root certificates?
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites Email
SSL Validation Type DV, OV, and/or EV	Do you perform identity/organization verification for all SSL certificates? Is it ever the case for SSL certs that the ownership of the domain name is verified, but the identity/organization of the subscriber is not verified?

EV policy OID(s)	Not requesting EV-enablement
CP/CPS	SITHS document repository: http://www.svrinfo.se/Projekt-tjanster/SITHS/Dokument-for-SITHS/ Certificates for Swedish Health and Social Care (HCC) (Swedish): http://www.svrinfo.se/VirtDocRoot%5CTj%C3%A4nster%5CSITHS%5CVisas%20p%C3%A5%20bolagswebb/02.%20Styrande%20dokument/HCC_Version_2_34.pdf SITHS Certificate Policy (Swedish): http://www.svrinfo.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.svrinfo.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.svrinfo.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)
Identity Verification	Please provide the document URLs and section numbers, which establish the procedures and policies for verifying the identity of the certificate subscriber.

	Information already provided: 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 The company's ownership of the domain name (the cn of the certificate is based on DNS name standard) is checked using the service of the Internet Infrastructure Foundation at www.iis.se (.se domain names are obtained from IIS) Personal certificate (hard certificate): · The key owner must sign the order used for production/issuing of the personal certificate. This is done using a signed e-mail or similar. · When receiving the certificate the key owner must be present and prove his/her identity using a valid and accepted identity document. · As an option the RA/LRA may confirm the identity of key owner if he/she knows the key owner. Two additional roles called ORA (similar to LRA but less local) and CRA (Card RA) also have rights to confirm the identity of the key owner. · The identity of the key owner may also be confirmed by another person, working within the organization of the key owner.
Domain Name Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate *or* has been authorized by the domain registrant to act on the registrant's behalf; Please provide the document URLs and section numbers, which establish the procedures and policies for verifying that the certificate subscriber owns/controls the domain name to be included in the SSL certificate. Please also provide translations into English.
Email Address Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to act on the account holder's behalf; If you are planning to request that the Email(S/MIME) trust bit be enabled, please provide the document URLs and section numbers, which establish the procedures and policies for verifying that the certificate subscriber

	owns/controls the email address to be included in the certificate. Please also provide translations into English.
Identity of Code Signing Subscriber	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for certificates to be used for digitally signing code objects, the CA takes reasonable measures to verify that the entity submitting the certificate signing request is the same entity referenced in the certificate *or* has been authorized by the entity referenced in the certificate to act on that entity's behalf; If you are planning to request that the Code Signing trust bit be enabled, please provide the document URLs and the section numbers which establish the procedures and policies for Code Signing certificates. Please also provide translations into English.
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information: related document URLs and section numbers, and translations into English of the relevant documentation. • Long-lived DV certificates o • Wildcard DV SSL certificates o • Delegation of Domain / Email validation to third parties o • Issuing end entity certificates directly from roots o • Allowing external entities to operate unconstrained subordinate CAs o • Distributing generated private keys in PKCS#12 files o • Certificates referencing hostnames or private IP addresses o • Issuing SSL Certificates for Internal Domains o • OCSP Responses signed by a certificate under a different root o • CRL with critical CIDP Extension o • Generic names for CAs o The name is not generic – has SITHS in it.