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	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 / 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? Please see https://wiki.mozilla.org/CA:SubordinateCA_checklist
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.inera.se/Infrastrukturtjanster/SITHS/Dokument-for-SITHS/ Certificates for Swedish Health and Social Care (HCC) (Swedish): http://www.inera.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.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)
Identity 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 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. -- Each RA has an RA-policy Practice Statement (RAPS), which provides details about how the SITHS Registration Authority Policy applies within their organization. Google Translation of section 3.1 of SITHS-RA-Policy 3.1 IDENTIFICATION OF REGISTRATION 3.1.1 GENERAL With regard to identification and authentication in order to HCC RA shall follow the CA's policy, section 3.1. The initial order of organization of its right to a domain name, the right to license, right to order and receive the certificate must always be verified by independent sources. Results and the verification approach must be documented and archived. 3.1.2 IDENTIFIERINGSPROCEDUR conducted by RA / ORA / LRA / KRA RA / ORA will ensure that procedures are described and defined on: · Control of qualified buyers of certified · establishing a basis for ordering certificates · extradition and blocking of certificates. RA / ORA / LRA shall establish a basis for ordering certificates verifying the proper application decided of the accountable. KRA shall establish a basis for ordering cards verified against the appropriate application adopted by the business manager. The certificate request is made identity as one of the following procedures: · HCC in person by personal presence and with the eID card as input for the first time of ordering of a license, subsequent license orders need not be any personal identification because the person is known electronically · at HCC HCC Organization and Function by personal attendance of the representative who approved and show valid identification document at the first opportunity, with subsequent certificate orders not needed any personal identification because the person is known electronically 3.1.3 REQUIREMENTS FOR PERSONAL ATTENDANCE RA / ORA extradite private keys, and the relevant password or PIN numbers at HCC and Organization HCC function. The disclosure is made in person to the authorized representative on presentation of an approved and valid identification, or by e-mail using S / MIME. Authorised Representative must have a valid HCC Privacy. These procedures are detailed in RAPS. 3.1.4 Authentication OF ORGANIZATION AND FUNCTION WITHIN A STRUCTURE When ordering a certificate of type HCC HCC Organization and Function, and its distribution private keys and codes attached to them, should there be a request by authorized representatives of organization. The initial order of organization of its right to a domain name, the right to license, right to order

	and receive the certificate must always be verified by independent sources. Results and the verification approach must be documented and archived. These procedures are detailed in RAPS. Google Translation of section 3.1 of SITHS-CA-Policy 3.1 INITIAL REGISTRATION 3.1.1 NAME TYPES Key Holders recorded with contact details and identity information. Verification of personal items implemented at each new order and updated at least annually at the internal audit work. The information about the key holder that is published in the issued certificate is a selection of the following Attribute: · Country · Regions · Organization · Organizational Unit · First name · Last Name · Full name in accordance with the key holder's normal use of presentation · A unique identifier · Service Title · Roll Name · Name of service / function · e-mail address (SMTP or X.400) · EDI address 3.1.1.1 HCC Privacy From the above, the following attributes occur in HCC Person: · Country · Regions · Organization · Organizational Unit · First name · Last Name · Full name in accordance with the key holder's normal use of presentation · A unique identifier · Function Name · e-mail address (SMTP or X.400) · EDI address 3.1.1.2 HCC Organization

	From the above, the following attributes occur in HCC Organization: · Country · Regions · Organization · Organizational Unit · A unique identifier · e-mail address (SMTP or X.400) · the EDI address 3.1.1.3 Function HCC From the above, the following attributes occur in HCC Function: · Country · Regions · Organization · Organizational Unit · A unique identifier · Function Name · e-mail address (SMTP or X.400) · EDI address 3.1.2 REQUIREMENTS OF NAME-VALIDITY If the attribute Country appears to specify that the country in which the importance of other attributes are defined and should be interpreted. This means then that all required attributes must be defined and could be interpreted in the same country. E-mail address can be both X.400 address as the address of the SMTP (RFC 822 names). Unique Identifier is a public identifier must be other than Swedish personal identity. Its primary purpose is to provide a unique identity for the functioning of information systems that can not be apply the identities composed of several attributes, but it must also ensure that two key holders not certified with the same identity. Organization name is officially registered organization's name in the specified country. For organization name registered in Sweden, the organization name must be registered with Swedish Patent and Registration Office. Organizational Unit is arbitrary designation on unit or branch of the organization. Name of organizational unit specified arbitrarily by the responsible organization which is also responsible for the name is unique within the organization for the specified country. The key holder's identity is specified by an arbitrary combination of attributes in 3.1.1 as long as combination includes the required attributes, and provides an unmistakable identity. An unmistakable identity is defined here as a set of attributes in an unmistakable way related to one specific person. The unmistakable link between identity and the person may depend on contexts in which concepts of identity management. Some of these circumstances may require help from current record holder (as when using e-mail address). 3.1.3 The authentication of the organizations belonging to

	Key holders affiliation must be certified (authorized) by an authorized representative for that organization. An authorization may represent one or more key holders. Authorised Representative, RA, working under the RA policy [RA-policy] is specified in the agreement under 09.02 signed by the current organization. The agreement shows that the organization is required to report relevant changes in circumstances relevant to the decision to freeze the certificate. 3.1.4 Authentication of individual IDENTITY Key Holders for which the authorized representative (employers, etc.) applying for certificates identified in ordering under 3.1.4.1 below. Alternatively designated contact officer who accepts an application, a test of the requesting meets the requirements for obtaining the type of license applied. Approval of application may be paid at time of application, which indicates the controller client identification and signing with digital signature to an identity check done. Approval may also be done before the time of application, whereby identity verification is logged separately as it performed. 3.1.4.1 Requirements for identity verification Identity check is made to any of the following procedures. a) The key holder showing approved and valid identification document. b) Key Holder legitimize themselves and sign your order electronically using an electronic ID document at least the equivalent level of safety in this certificate policy. 3.1.4.2 Procedure for authentication Before the certificate is created so checked all the key holder's identity, which is not exceptional below, the HSA [HSA]. 3.1.4.3 Requirements for personal presence Electronic identity verification when ordering the certificate does not require the personal attendance of the key holder. Other identity checks when ordering by face to face. 3.1.5 Authentication of organizations and functions of the organization When ordering a certificate of type HCC HCC Organization and Function, and its distribution private keys and codes attached to them, called up a written order from an authorized representative for that organization. This order may relate to one or more key holders. 3.1.5.1 Authentication of the representative The extradition of private keys and codes are checking the identity of authorized representative. 3.1.5.2 Requirements for personal presence Ordering a certificate by written order from the agreements which do not require personal presence by the client. Identity check the extradition of private keys and codes require personal attendance by authorized representative at the time of delivery, the option is delivery of codes with S / MIME to the jurisdiction recipient of the order. If the authorized representative can not personally HCC HCC and Function HCC Organization delivered by e-mail if and only if the PINs are sent via other media, such as a Independent SMS text message.

	3.1.5.3 Verification of the right to the domain and certificates The initial order of organization of its right to a domain name, the right to license, right to order and receive certificates must always be verified by independent sources. Results and the verification approach must be documented and archived. 2.3 RENEWED REGISTRATION FOR RENEWAL OF KEYS Request for re-key pair and corresponding certificate for HCC HCC Organization and Function shall be as prescribed in 3.1. 3.3 RENEWED REGISTRATION FOR RENEWAL OF KEYS FOR LOCK Request for renewal of key pairs and related certificates of release of the Certificate of HCC Organization HCC and function shall be as prescribed in 3.1.
Domain Name Ownership / Control	Google Translation of SITHS-CA-Policy section 3.1.5.3, Verification of the right to the domain and certificates: The initial order of organization of its right to a domain name, the right to license, right to order and receive certificates must always be verified by independent sources. Results and the verification approach must be documented and archived. Comment #3: Functional/organizational certificate (soft certificate): 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) In order to meet the requirements of section 7 of the Mozilla CA Certificate Policy, more information needs to be provided in a publicly-available and audited document (such as the CP) which describes the steps that must be taken by the RA to verify that the certificate subscriber owns/controls the domain name to be included in the certificate. The information in section 3.1.5.3 of the SITHS-CA-Policy is too high level; more details need to be provided. The information provided in comment #3 about using a service to get data from a third party about the owner of the domain name is better, but still not quite enough detail. For instance, what information is collected from www.iis.se and compared with the information provided by the certificate subscriber? Is the RA required to perform any other checks in order to confirm that the certificate subscriber owns/controls the domain name to be included in the certificate? Please see: https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership
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	If you are planning to request that the Code Signing trust bit be enabled, please provide the document URLs and section numbers, which establish the procedures and policies that are specific to code signing certificates.

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
	  ○
	• Wildcard DV SSL certificates
	  ○
	• Email Address Prefixes for DV SSL Certs
	  ○
	• Delegation of Domain / Email validation to third parties
	  ○
	• Issuing end entity certificates directly from roots
	  ○
	• Allowing external entities to operate unconstrained 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
	  ○