Bugzilla ID: 562763
Bugzilla Summary: Add SafeScrypt 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	SafeScrypt (Sify)
Website URL	http://www.safescrypt.com/
Organizational type	Private
Primary market / customer base	Sify Communications Data Security Solutions primary focus is on providing Digital Trust Services and high-end solutions – that help businesses migrate to an environment that is secure and enables compliance with Legal and Regulatory requirements for true, end-to-end electronic transactions and overall E-Business. Sify Communications is also India's first intermediate CA under the IT Act 2000 and a VeriSign Affiliate for the Indian Subcontinent offering Managed PKI services to enterprises and Digital Certificates to end-users as well Sify primarily serves Government, Semi-Government, and Private orgranizations in India.
CA Contact Information	CA Email Alias: practices@safescrypt.com CA Phone Number: 91-044-22540770 Title / Department: Certificate Practices

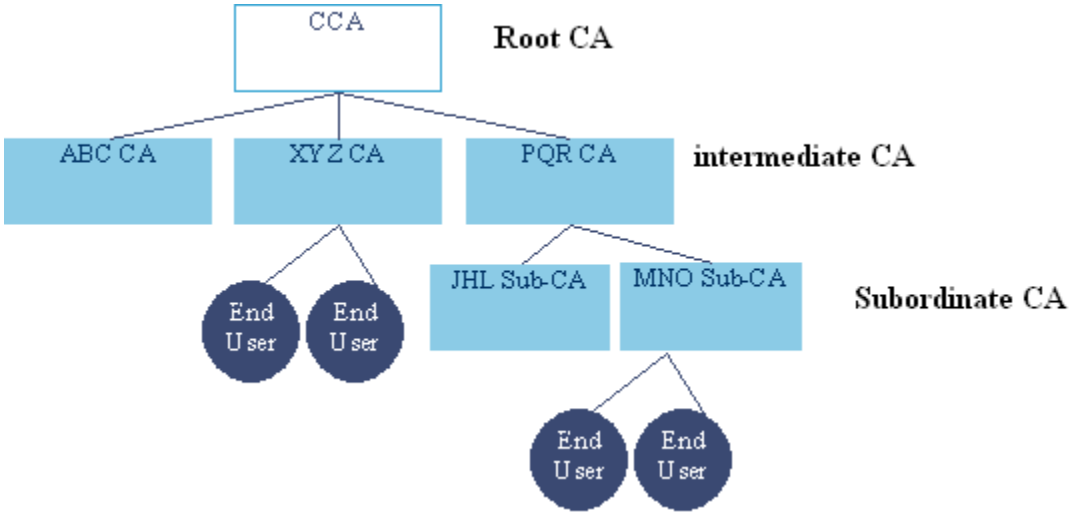
SafeScrypt has 3 sub-CAs that are signed by the "CCA India 2007" root certificate. CCA submitted a request for inclusion of the root certificate in bug #557167. Upon reviewing the request it was determined that the size and complexity of the hierarchy was such that each sub-CA would need to be separately evaluated. https://bugzilla.mozilla.org/show_bug.cgi?id=557167#c16

CPS Section 1.0.2.2: The SafeScrypt India-RCAI Public Hierarchy refers to that CA hierarchy from SafeScrypt that is cross certified with the Root CA Authority of India (RCAI). This root is envisaged to serve as the basis for cross-certification amongst various licensed CA's in India for consumer applications. Under this hierarchy, the following Classes of Certificates are available:

- India-RCAI Class 1
  - This Class 1 CA root certificate is not activated, and it has not signed any sub-CAs or end-entity certificates. SafeScrypt is not requesting inclusion of this root at this time.
- India-RCAI Class 2
- India-RCAI Class 3

	Safescrypt India-RCAI Class 2 CA-G2	**Safescrypt India-RCAI Class 3 CA-G2**
Cert summary	This Class 2 CA has signed 10 subCAs, which sign end-entity certs. Certificates signed by this CA are issued to individuals, including members of the general public.	This Class 3 CA and has signed one subCA, which signs end-entity certs. Certificates signed by this CA are issued to: • Individuals, including members of the general public. • Individuals serving in the role of Administrator (Trusted Persons who perform Certificate or certification service management functions on behalf of SafeScrypt, Managed PKI Customers, or trusted fourth parties). • Organizations that control a device include, but are not limited to: Web servers or web traffic management devices (Secure Server IDs and Global Server IDs), Electronic Data Interchange servers, OFX servers, Devices digitally signing code or other content. • Organizations that control multiple web servers, for which Managed PKI Administrator of such organization approve the issuance of Secure Server IDs and/or Global Server IDs.
Impact to Mozilla Users	Please provide a statement about what sorts of Mozilla Users will benefit from the inclusion of this sub-CA as a trust-anchor in NSS.	Please provide a statement about what sorts of Mozilla Users will benefit from the inclusion of this sub-CA as a trust-anchor in NSS.
Root Cert URL	http://cca.gov.in/rw/pages/download_certificate.en.do?id=Safescrypt%20India-RCAI%20Class%202%20CA-G2&year=2007	http://cca.gov.in/rw/pages/download_certificate.en.do?id=Safescrypt%20India-RCAI%20Class%203%20CA-G2&year=2007
SHA-1 fingerprint	5D:04:0E:E7:FB:6D:C0:BC:01:58:B6:F2:9E:4B:C0:45:D4:18:A6:87	D3:79:BB:52:95:6D:6E:51:38:D2:25:4D:92:5E:48:2A:1C:4B:8E:CF
Valid from	2007-07-09	2007-07-09
Valid to	2015-07-03	2015-07-03
Cert Version	3	3
Modulus length	2048	2048
Test Cert	Please provide a test cert that chains up to this sub-CA.	Please provide a test cert that chains up to this sub-CA.
CRL URL	http://crl.safescrypt.com/RCAIClass2.crl The CRL will be updated once in 24 hours for end entity certificates.	http://crl.safescrypt.com/RCAIClass3.crl The CRL will be updated once in 24 hours for end entity certificates.
OCSP Responder	http://ocsp.safescrypt.com	http://ocsp.safescrypt.com
SafeScrypt CA Hierarchy	"Safescrypt India-RCAI Class 2 CA-G2" has the following internally operated sub-CAs, which sign end-entity certificates for signing and encryption. 1. BarclaysBankPLCCA validity: 15/05/2008 to 14/05/2013	"Safescrypt India-RCAI Class 3 CA-G2" has the following internally operated sub-CA which signs end-entity certificates for signing and encryption: 1. Safescrypt India-RCAI Class 3 Consumer CA validity: 21/02/2003 to 03/07/2014

	2. C1IndiaCA validity: 29/09/2007 to 28/09/2012 3. ColumbiaAsiaHospitalsPvtLtdRCAIC2CA validity: 15/05/2008 to 14/05/2013 4. NSE.ITRCAIClass2CA validity: 31/03/2006 to 02/07/2014 5. tendertimes.comCA validity: 06/03/2007 to 02/07/2014 6. SafescryptEngineeringCA validity: 09/07/2007 to 08/08/2012 7. DGFTOnlineCA validity: 21/02/2003 to 04/07/2014 8. SafescryptRCAIClass2ConsumerIndividualSubscriberCA validity: 16/09/2005 to 19/05/2012 9. SafescryptRCAIClass2OnSiteIndividualSubscriberCA validity: 20/05/2005 to 19/05/2012 10. ContainerCorporationofIndiaLimitedCA validity: 01/03/2007 to 02/07/2014	
Externally Operated subCAs	All the Sub-CAs are operated by Safescrypt.	All the Sub-CAs are operated by Safescrypt.
Cross-signing	None	None
Requested Trust Bits	Email (S/MIME)	Email (S/MIME)
SSL Validation Type	Not Applicable. SSL certs are not signed under this sub-CA.	Not Applicable. SSL certs are not currently signed under this sub-CA.
EV policy OID	Not requesting EV enablement for this root.	Not requesting EV enablement for this root.
CCA CA Hierarchy	In order to facilitate greater flexibility to Certifying Authorities, the CCA allowed the creation of subordinate-CAs. As per this model, an intermediate Certifying Authority can create a subordinate-CA to meet his business-branding requirement. However the subordinate-CA will be part of the same legal entity as the CA. It is also necessary that the subordinate-CA will be in the same infrastructure of intermediate CA. The CA model will be based on the following principles (effective from Jan 2011) • The intermediate CAs MUST NOT have more than ONE level of subordinate -CAs • The subordinate-CA MUST use a subordinate-CA certificate issued by the intermediate CA for issuing end entity certificates • The subordinate-CA must necessarily use the intermediate-CAs infrastructure for issuing certificate • The subordinate-CAs operations shall be subject to same audit procedures as the intermediate CA • The certificate policies of the subordinate-CA must be same as of the intermediate CA's certificate policies	

	 There are currently seven intermediate CAs under the Root CA of India. Though intermediate CAs have subordinate CA under that, they are all physically located in the same physical infrastructure of intermediate CAs. The subordinated CAs are allowed mainly for operational management. The intermediate CAs and its subordinate CAs have single CPS. The Audit is as per security guidelines mentioned in the Information Technology ACT. Strict measures are taken by Root CA to monitor the compliance of CPS, and recommendations specified in the Information Technology Act Framework Diagram: https://bugzilla.mozilla.org/attachment.cgi?id=436978
CCA CP/CPS	Root CA CPS: http://cca.gov.in/rw/pages/rcai_cps.en.do Steps to become CA: http://cca.gov.in/rw/pages/becoming_ca_suppdoc.en.do FAQ : http://cca.gov.in/rw/pages/faqs.en.do CCA sub-CAs: http://cca.gov.in/rw/pages/ca_certificates_2007.en.do
SafeScrypt CP/CPS	CPS (English): http://www.safescrypt.com/pdf/cps.pdf The CPS covers practices and procedures concerning the issuance and management of all Certificate Classes within each hierarchy of SafeScrypt. Additional information provided by SafeScrypt: https://bugzilla.mozilla.org/attachment.cgi?id=436984

	CPS Section 1.9.3.2: The SafeScrypt India-RCAI Public Hierarchy is based on the RCAI Certificate Policy ("RCAI CP"). More information concerning the RCAI CP is available at http://www.safescrypt.com/cp.
AUDIT	CPS section 2.7: SafeScrypt performs regular audits, annual as well as half yearly and quarterly, in compliance with the Specifications in the IT Act 2000, as its associated rules and regulations. These audits are performed by an auditor empanelled with the Controller of Certifying Authorities (CCA), Govt. of India. This audit is performed for SafeScrypt's data center operations and key management operations supporting SafeScrypt's public and Managed PKI services. Customer-specific CAs are not specifically audited as part of the audit of SafeScrypt's operations unless required by the Customer or any other authority under the IT Act 2000. SafeScrypt shall be entitled to require that Managed PKI Customers undergo a compliance audit under this CPS § 2.7 and audit programs for these types of Customers. CPS section 2.7.3: Compliance audits of SafeScrypt's operations are performed by an auditing firm that is independent of SafeScrypt. Audit Type: WebTrust CA Equivalent Auditor: Qadit Systems Auditor Website: http://www.qadit.com Audit Document URL(s): Confidential CCA Approved Auditors List: http://cca.gov.in/rw/pages/auditors.en.do CCA Audit Criteria: http://cca.gov.in/rw/pages/auditors_auditcriteria.en.do Information Technology Act: http://cca.gov.in/rw/pages/it_act.en.do Rules: http://cca.gov.in/rw/pages/rules.en.do Act Modification: http://cca.gov.in/rw/resource/actmod_nov02.pdf IT Act Regulations: http://cca.gov.in/rw/pages/regulations.en.do As per the Mozilla CA Certificate Policy (http://www.mozilla.org/projects/security/certs/policy/) we will need a document from the auditor stating which criteria that was used to audit these sub-CAs, that the criteria is equivalent to WebTrust CA, and the dates during which the most recent audit was performed.
Organization Identity Verification	CPS sections 3.1.8 and 3.1.9 document procedures for authentication of the Organization Identity and Individual Identity. CPS section 1.1.1.b: **India-RCAI Class 1 Certificates:** They offer the lowest level of assurances within the SafeScrypt India--RCAI Public hierarchy. They are individual Certificates, whose validation procedures are based on assurances that the Subscriber's distinguished name is unique and unambiguous within the sub CA's Subdomain and that a certain e-mail address is associated with a public key. They are appropriate for digital signatures, encryption, and access control for non-commercial or low-value transactions where proof of identity is unnecessary. **SafeScrypt India-RCAI Class1 certificates do not validate the identity of the subscriber and therefore are not Persona-verified Digital Signature Certificates**

	India-RCAI Class2 Certificates: They offer a medium level of assurances in comparison with the other two Classes in this hierarchy. Again, they are individual Certificates. In addition to the India-RCAI Class 1 validation procedures, India--RCAI Class 2 validation procedures add procedures based on a comparison of information submitted by the Certificate applicant against information in business records or databases or the database of a SafeScrypt-approved identity proofing service. ***SafeScrypt reserves the sole right to approve the database or record being used for this validation.*** They can be used for digital signatures, encryption, and access control, including as proof of identity in transactions. ***This class is suitable for most business-grade transactions*** **India-RCAI Class 3 Certificates:** This class of certificates provides the highest level of assurances within the India-RCAI hierarchy. India-RCAI Class 3 Certificates are issued to individuals, organizations, and Administrators for CAs and RAs. India-RCAI Class 3 individual Certificates may be used for digital signatures, encryption, and access control, including as proof of identity, in high-value transactions. India-RCAI Class 3 individual Certificates provide assurances of the identity of the Subscriber based on the personal (physical) presence of the Subscriber before a person ***(approved by SafeScrypt)*** that confirms the identity of the Subscriber using, at a minimum, a well-recognized form of government-issued identification and one other identification credential. ***SafeScrypt reserves the right to decide which specific forms of identification would be acceptable for validation. In the absence of a government-issued identification, SafeScrypt may prescribe alternate methods of validation.*** Other India-RCAI Class 3 organizational Certificates are issued to devices to provide authentication; message, software, and content integrity; and confidentiality encryption. India-RCAI Class 3 organizational Certificates provide assurances of the identity of the Subscriber based on a confirmation that the Subscriber organization does in fact exist, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Subscriber was authorized to do so. CPS section 3.1.8: SafeScrypt confirms the identity of India Class C, India -RCAI Class 3 and VTN Class 3 organizational end-user Subscribers and other enrolment information provided Certificate Applicants (except for Non-verified Subscriber Information) in accordance with the procedures set forth in the subsections that follow. In addition to the procedures below, the Certificate Applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate in accordance with CPS § 3.1.7.
Domain Name Ownership / Control	Not Applicable. Not requesting enablement of websites trust bit. For VTN server certificates, SafeScrypt verifies that the certificate applicant is the record owner of the domain name of the server that is the Subject of the Certificate or is otherwise authorized to use the domain. Does this statement apply to India-RCAI Class3? Currently we are not issuing any SSL certificates under this Sub-CA.
Email Address Ownership / Control	CPS Table 2: ***India-RCAI Class 1*** **Applicant Verification:** Name and e-mail address search to ensure that the distinguished name is unique and unambiguous within the CA's Subdomain.

	Use: Modestly enhancing the security of e-mail through confidentiality encryption, digital signatures, and web-based access control, where proof of identity is unnecessary. Applications requiring a low level of assurances in comparison with the other Classes, such as noncommercial web browsing and email. ***India-RCAI Class 2*** **Applicant Verification:** Same as India-RCAI Class 1 Retail, plus automated or Administrator-initiated enrolment information check with one or more third-party databases or comparable sources. **Applicant Verification:** Same as India-RCAI Class 1 Managed PKI plus checking internal documentation or databases to confirm identity of the Certificate Applicant (*e.g.*, human resources documentation). **Use:** Enhancing the security of e-mail through confidentiality encryption, digital signatures for authentication, and web based access control. Applications requiring a medium level of assurances in comparison with the other Classes, such as some individual and intra- and intercompany e-mail, on-line subscriptions, online banking or stock trading, supply chain management & account applications, and password replacement, including as proof of identity for medium-value transactions. . Generally used for most Business Grade transactions CPS section 3.1.9 describes the procedures for verifying the identity of the certificate subscriber. ***India-RCAI Class 3*** **Applicant Verification:** Same as India-RCAI Class 1 Retail, plus personal presence and check of two or more ID credentials. **Use:** Enhancing the security of e-mail through confidentiality encryption, digital signatures for authentication, and web based access control. Applications requiring a high level of assurances in comparison with the other Classes, such as some online banking, corporate database access, and exchanging confidential information, including as proof of identity for high-value transactions. **Applicant Verification:** Check of third-party database or other documentation showing proof of right to use the organizational name. Validation check by telephone (or comparable procedure) to confirm information in, and authorization of, the Certificate Application **Use:** Server authentication, confidentiality encryption, and (when communicating with other servers) client authentication, message integrity; and authentication and integrity of software and other content. Please see https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control There needs to be public-facing and audited documentation (such as in the CPS) about steps that are taken to verify that the certificate subscriber owns/controls the email address to be included in the certificate.	
Identity of Code Signing Subscriber	Not Applicable.	Not Applicable.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  ○ Not enabling websites trust bit.
	• Wildcard DV SSL certificates
	  ○ Not enabling websites trust bit.
	• Delegation of Domain / Email validation to third parties
	  ○ ?	

	• Issuing end entity certificates directly from roots
	  ○ No.
	• Allowing external entities to operate unconstrained subordinate CAs
	  ○ No.
	• Distributing generated private keys in PKCS#12 files
	  ○ ?
	• Certificates referencing hostnames or private IP addresses
	  ○ Not enabling websites trust bit.
	• Issuing SSL Certificates for Internal Domains
	  ○ Not enabling websites trust bit.
	• OCSP Responses signed by a certificate under a different root
	  ○ ?
	• CRL with critical CIDP Extension
	  ○ CRLs import into a Firefox browser without error.
	• Generic names for CAs
	  ○ Name includes Safescrypt.