Bugzilla ID: 662259
Bugzilla Summary: SG Trust services Root certificate

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	SG Trust Services
Website URL	http://www.sgtrustservices.com/en/index.htm
Organizational type	Indicate whether the CA is operated by a private or public corporation, government agency, international organization, academic institution or consortium, NGO, etc. Note that in some cases the CA may be of a hybrid type, e.g., a corporation established by the government. For government CAs, the type of government should be noted, e.g., national, regional/state/provincial, or municipal.
Primark Market / Customer Base	Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does the CA focus its activities on a particular country or other geographic region?
Impact to Mozilla Users	Describe the types of Mozilla users who are likely to encounter your root certificate as relying parties while web browsing (HTTPS servers doing SSL), sending/receiving email to their own MTA (SMTPS, IMAPS servers doing SSL), sending/receiving S/MIME email (S/MIME email certs), etc.
CA Contact Information	CA Email Alias: CA Phone Number: Title / Department:

Technical information about each root certificate

Certificate Name	SG TRUST SERVICES RACINE

Certificate Issuer Field	CN = SG TRUST SERVICES RACINE
	OU = SG TRUST SERVICES
	O = GROUPE SG
	What is "Groupe SG"?

Certificate Summary	A summary about this root certificate, it's purpose, and the types of certificates that are issued under it.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=537544
SHA1 Fingerprint	A1:1F:B9:2D:BE:35:C9:21:C1:EA:99:B1:EB:FA:2C:43:E3:EE:84:89
Valid From	2003-07-22
Valid To	2023-07-22
Certificate Version	3
Certificate Signature Algorithm	PKCS #1 SHA-1 With RSA Encryption

Signing key parameters	2048
Test Website URL (SSL) Example Certificate (non-SSL)	If you are requesting to enable the Websites (SSL/TLS) trust bit, please provide the URL to a website whose SSL cert chains up to this root. Note that this can be a test site.
CRL URL	URL NextUpdate for CRLs of end-entity certs, both actual value and what's documented in CP/CPS. Test: Results of importing into Firefox browser
OCSP URL	OCSP URI in the AIA of end-entity certs Maximum expiration time of OCSP responses Testing results a) Browsing to test website with OCSP enforced in Firefox browser b) If requesting EV: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
Requested Trust Bits	One or more of: Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	e.g. DV, OV, and/or EV
EV Policy OID(s)	

CA Hierarchy information for each root certificate

CA Hierarchy	List, description, and/or diagram of all intermediate CAs signed by this root. Identify which subCAs are internally-operated and which are externally operated.
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 If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.
Cross-Signing	List all other roots for which this root CA has issued cross-signing certificates. List all other root CAs that have issued cross-signing certificates for this root CA. Note whether the roots in question are already included in the Mozilla root store or not.

Verification Policies and Practices

Policy Documentation	Language(s) that the documents are in. CP URL: CPS URL: Relying Party Agreement URL: (Please provide URLs to the current versions of these documents on your website. Also please provide English versions if available.)
Audits	Audit Type: ETSI 102 042 Auditor: LSTI Auditor Website: http://www.lsti-certification.fr/ (Please provide the URL to the ETSI certificate for SG Trust Services on the LSTI website.)

	URL to Audit Report and Management's Assertions: https://bugzilla.mozilla.org/attachment.cgi?id=537541 Date of completion of last audit: 2011.05.11
SSL Verification Procedures	If you are requesting to enable the Websites Trust Bit, then provide (In English and also the original text 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 also the original text 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 also the original text in publicly available documentation) all the information requested in #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

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	