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 http://www.societegenerale.com/
Organizational type	SG Trust Services is a subsidiary of Groupe SG, which is the high level entity of all subsidiaries of Société Générale. Société Générale is one of the oldest and largest banks in France, and is a major international financial services company.
Primark Market / Customer Base	Customers are general publics who make e-Services with banks and French government third parties.
Impact to Mozilla Users	The types of Mozilla users who are likely to encounter your root certificate as relying parties are the general public in France.
CA Contact Information	CA Email Alias: Sgtrust.Services@socgen.com, Joël Dupont <joel.dupont@socgen.com> CA Phone Number: 01 42 14 54 63 Title / Department: Chief of SG Trust Services CA (Responsable de l'Offre Certificats Electroniques)

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
Certificate Summary	SG TRUST SERVICES RACINE has two internally-operated intermediate certificates, one for authentication certificates and another for signing certificates.
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
Cert Signature Algorithm	PKCS #1 SHA-1 With RSA Encryption
Signing key parameters	2048
Example Certificate (non-SSL)	https://bugzilla.mozilla.org/attachment.cgi?id=544773 We attached you users' certificate (authentication and singing) : the private key password is : #SGTS2011.

CRL URL	http://crl.sgtrustservices.com/SGTS-2Etoiles/LatestCRL When I try to import this CRL into my Firefox browser, I get the following error. The application cannot import the Certificate Revocation List (CRL). Error Importing CRL to local Database. Error Code:ffffe009 ffffe009 is equivalent to -8183, "Security library: improperly formatted DER-encoded message." It means that the reply contained anything other than a valid DER-encoded CRL. Typical Resolution: Change encoding from PEM to DER. Please see #13 of https://wiki.mozilla.org/CA:Information_checklist#Technical_information_about_each_root_certificate
OCSP URL	None
Requested Trust Bits	Email (S/MIME) Comment #9: Certificate issued by "SG TRUST SERVICES RACINE" root certificate are for authentication and signature usages. So we only need the email trust bit to be active.
SSL Validation Type	IV
EV Policy OID(s)	Not EV

CA Hierarchy information for each root certificate

CA Hierarchy	SG TRUST SERVICES RACINE has two internally-operated intermediate certificates, one for authentication certificates and another for signing certificates. I see that one of the intermediate certs has CN=SG TS 2 ETOILES What is the CN of the other intermediate cert?
Externally Operated SubCAs	Does this root currently have (or may it have in the future) subCAs that are operated by external third parties?
Cross-Signing	Has this root been involved in cross-signing with any other root certificate? 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	Documents Repository: http://www.sgtrustservices.com/entreprise/pc/index.htm CP for Authentication and Encryption Certs (French): http://www.sgtrustservices.com/entreprise/pc/authentification/index.htm CP for Signing Certs (French): http://www.sgtrustservices.com/entreprise/pc/signature/index.htm
Audits	Audit Type: ETSI 102 042 Auditor: LSTI Auditor Website: http://www.lsti-certification.fr/

	ETSI Certificate: https://bugzilla.mozilla.org/attachment.cgi?id=537541 (2011.05.11) On LSTI website: http://www.lsti-certification.fr/images/stories/listergs_07032011.pdf (Last page, audited to RGS V1.0, SG TS 2ETOILES for authentication and signature)
SSL Verification Procedures	N/A. Not requesting the website trust bit.
Organization Verification Procedures	Translations from CP (These sections appear to be the same in both documents). (Please correct the translations as needed) 3.1.1. Information carried in the "Subject" field of the Certificate The information contained in the "Subject" field ("Subject" in English) of the Certificate described below explicitly: • the first name and surname of the bearer will be found in CN ("Common Name") PrintableString X.501 format. This information is contained in those documents submitted by the Subscriber in the subscription; • e-mail address (e-mail) of the Carrier; • the name, the SIREN number (or if the registration to another public record) that appears on the Subscription Agreement, the name of the town and country (according to the international convention of naming) of the seat office of the employer of the holder, as shown on the Individual Subscriber Request endorsed by the Certificate Manager. • The DN Qualifier 3.1.5 Verifying the identity of the Customer, the Certificate Manager and Carrier The verification of the identity of the customer is the responsibility of the Distributor. Verifies that - according to the rules and practices applicable in the matter - that the documents produced by the Representative is capable of establishing the existence and identity of the client and the identity and authority of the Representative. The verification of the identity of the Certificate Manager is the responsibility of Distributor. Verifies that - according to the rules and practices applicable in the matter - that the documents produced by the Certificate Manager is required to establish its existence and identity. The verification of the identity of the wearer is the responsibility of the Certificate Manager. Prior to the submission of the dossier to a Distributor, Manager of Certificates will: • verify that the applicant is a holder of certificate authorized to use certificates on behalf of the Client; • Collect all documents relating to the bearer, check their authenticity and to make a photocopy, signed by the carrier and by itself; • check the accuracy of statements that establish the identity of the bearer; • affix his signature on the back of each photocopy. Certificate Manager agrees to carry out the checks described above independently and with integrity.
Email Address Verification Procedures	CA is qualified to RGS level two stars. Comment #6: Subscribers must provide complete registration information. To obtain a cryptographic support and install their certificate, they must meet a registration operator who checks the identity paper of the subscriber.

	Where is it documented how the RA must verify that the certificate subscriber own/controls the email address to be included in the certificate? Please provide the URLs, section numbers, and English Translations of the relevant documents. If this information is in the RGS documentation, please still provide the URLs, section numbers, and translations into English. Mozilla CA Certificate Policy: http://www.mozilla.org/projects/security/certs/policy/InclusionPolicy.html "6. We require that all CAs whose certificates are distributed with our software products: + provide some service relevant to typical users of our software products; + publicly disclose information about their policies and business practices (e.g., in a Certificate Policy and Certification Practice Statement);" and "7. We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: + all information that is supplied by the certificate subscriber must be verified by using an independent source of information or an alternative communication channel before it is included in the certificate; + for a certificate to be used for digitally signing 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;"
Code Signing Subscriber Verification Procedures	N/A. Not requesting the code signing trust bit.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes
CA Hierarchy	OK
Audit Criteria	OK
Document Handling of IDNs in CP/CPS	CP section 3.1.2: all characters are PrintableString format, ie without accents or characters specific to the French language and to conform to the X.501 standard;
Revocation of Compromised Certificates	??? See item #2 of http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html
Verifying Domain Name Ownership	N/A
Verifying Email Address Control	See above.
Verifying Identity of Code Signing Certificate Subscriber	N/A
DNS names go in SAN	N/A
Domain owned by a Natural Person	N/A
OCSP	N/A

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	N/A – not requesting websites trust bit.
Wildcard DV SSL certificates	N/A
Email Address Prefixes for DV Certs	N/A
Delegation of Domain / Email validation to third parties	Can external third parties perform the verification of ownership/control of the email address to be included in the certificate?
Issuing end entity certificates directly from roots	No. EE certs are only signed by intermediate certs, not root.
Allowing external entities to operate subordinate CAs	???
Distributing generated private keys in PKCS#12 files	???
Certificates referencing hostnames or private IP addresses	N/A
Issuing SSL Certificates for Internal Domains	N/A
OCSP Responses signed by a certificate under a different root	N/A
CRL with critical CIDP Extension	??? – CRL doesn't import into my Firefox browser.
Generic names for CAs	CN = SG TRUST SERVICES RACINE O = GROUPE SG "Groupe SG" is the high level entity of all subsidiaries of SG (Societe Generale). When I do an internet search of Groupe SG, the top hits are for http://www.societegenerale.com/
Lack of Communication With End Users	Contact info is provided in CP docs.