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	C = FR O = SG TRUST SERVICES OU = 0002 43525289500022 CN = SG TRUST SERVICES RACINE
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=608632
SHA1 Fingerprint	0C:62:8F:5C:55:70:B1:C9:57:FA:FD:38:3F:B0:3D:7B:7D:D7:B9:C6
Valid From	2010-09-06
Valid To	2030-09-05
Certificate Version	3
Cert Signature Algorithm	PKCS #1 SHA-256 With RSA Encryption
Signing key parameters	4096
Example Certificate (non-SSL)	https://bugzilla.mozilla.org/attachment.cgi?id=544773 We attached you users' certificate (authentication and signing) : the private key password is : #SGTS2011.

CRL URL	http://crl.sgtrustservices.com/racine-GroupeSG/LatestCRL http://crl.sgtrustservices.com/SGTS-2Etoiles/LatestCRL (NextUpdate: 6 days)
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.
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.
Externally Operated SubCAs	None
Cross-Signing	None
Technical Constraints on third party issuers	Not applicable

Verification Policies and Practices

Policy Documentation	Document 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 CP for 2-Star Certs (French): https://www.sgts.rgs2e.sgtrustservices.com/doc/PC/SG_TS_2E_PC_Authentification.pdf CP for 2-Star Certs (English translation of some sections): https://bugzilla.mozilla.org/attachment.cgi?id=560318
Audits	Audit Type: ETSI 102 042 Auditor: LSTI Auditor Website: http://www.lsti-certification.fr/index.php?option=com_content&view=article&id=54&Itemid=14 ETSI Certificate: https://bugzilla.mozilla.org/attachment.cgi?id=537541 Annual surveillance audits are performed. The last one was done in November 2011, and the next one is planned for December 2012. 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.
CAB Forum Baseline Requirements	Comment #65: "SG Trust CAs" are conforming to RGS** which is equivalent to ETSI 102042 NCP+. SG Trust updates their operations and documentation each year to be conformed to the ETSI. Moreover SG Trust confirms that they will update their operations and documentation accordance by Cabforum baseline requirements if the new requirements are compatible with ETSI 102042.

Organization Verification Procedures	CA is qualified for RGS level two stars. CP for 2-Star Certs Section 3.2.3.3 describes the steps to verify and register a Certificate Manager (the customer) English translations provided https://bugzilla.mozilla.org/attachment.cgi?id=560318 - The Legal Representative also signs the subscription contract between the organisation to which they belong (the Client) and SG Trust Services. - The Legal Representative must provide the future Manager with a "K-bis" certifying the company's registration with a French trade and companies register (or any similar trade register for foreign entities) or an identification certificate from the Répertoire National des Entreprises et de leurs Établissements database. Legal Representatives of an association must provide a copy of the Journal Officiel containing the mention of their organisation as well as a copy of its articles of association and the minutes of the last Annual General Meeting during which an executive was appointed. - The Customer account manager meets with the future CM in person and checks their proof of identity. - The Customer account manager validates the appointment of the Certificate Manager and verifies that: -- The Registration File is complete. -- The Legal Representative has signed the Certificate Manager Identification Form and the subscription contract. -- The future Certificate Manager has signed the Certificate Manager Identification Form. -- The information in the Certificate Manager Identification Form is consistent with both the ID card (for personal ID information) and the subscription contract (for the organisation's information).
Explanation of Certificate Manager (Comment #32)	Registration service is a group of person of SG Trust Services. Only Registration Operators, in the Registration Service (group of person of SG Trust Services formerly identified by Head of the CA) can approve certificate issuance. Certificate Manager is a person into a client company of SG Trust Services who can: - Collect the registration document (Individual Subscriber Request) of the Subscriber; - Valid the registration documents before sending to registration service; - Make sign Disclosure Statement to the Subscriber; Each Certificate Manager meets the registration service of SG Trust Service in face to face. The Legal Representative must provide the future Manager with a "K-bis" certifying the company's registration with a French trade and companies register (or any similar trade register for foreign entities) or an identification certificate from the "Répertoire National des Entreprises et de leurs Établissements" database. Legal Representatives of an association must provide a copy of the "Journal Officiel" containing the mention of their organization as well as a copy of its articles of association and the minutes of the last Annual General Meeting during which an executive was appointed. Registration Service validates each subscriber's registration demand by: - Validating that the Certificate Manager who provide the registration documents are well-known; - Validating the completion of registration documents; - Validating the copy of the subscriber's identity card; - Compare signature of disclosures statements and signature of the identity card.
Email Address Verification Procedures	Comment #32: The email address is provided by subscriber into the documents registration. The Certificate Manager verifies that the email is correct and is attached to his organization before sending to Registration Service. In technical process, only the subscriber can receive into the email declared on registration documents the install URL of his certificate.

	CA is qualified for RGS level two stars. CP for 2-Star Certs Section 3.2.3.4 describes the steps that the Certificate Manager (the customer) takes to register a certificate subscriber. English translations provided https://bugzilla.mozilla.org/attachment.cgi?id=560318 The following procedure is systematically applied: - The future Subscriber must bring the Certificate Manager his ID card. - The Certificate Manager verifies that the person present matches the ID card. - The Certificate Manager photocopies the proof of identity adding "Certified Copy" and signs it. The Subscriber also signs the photocopy of the ID card. - The Certificate Manager ensures that the future Subscriber is authorised to use the certificates on behalf of the Client. - The Certificate Manager asks the Subscriber to complete and sign the Individual Subscriber Request Form. He ensures that the identity information filled in by the Subscriber matches the information on the ID card. The Certificate Manager sends the registration file to the Customer account manager. The registration file of a new Subscriber includes: - The Individual Subscriber Request (ISR) form dated less than 3 months prior, completed and signed both by the future Subscriber and the CM. -- The ISR form includes personal information on the future Subscriber required for creating the certificate. -- The ISR form includes the General Terms and Conditions of Use. - The photocopy of the Certificate Subscriber's ID card, signed by the Certificate Manager and the Subscriber. 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.
Code Signing Subscriber Verification Procedures	N/A. Not requesting the code signing trust bit.
Multi-factor Authentication	Translation of CP section 2.4: Published datas are accessible in read mode to all people concerning by certificates signed by SG Trust Services (Internet Access). Adding, deleting and modifications are limited only to authorized persons defining by Head of the CA. Registration Operators and PKI's administrators can access data, including status of certificates (adding, deleting or modification process) by personal authentication certificate stored on SSCD, after obtaining a particular accreditation. Technical administrators of the publication web site can access data, including status of certificates (adding, deleting or modification process) by personal two-factor authentication, after obtaining a particular accreditation. Data transfer from PKI's administrators to Technical administrators of the publication web site is done throw a secured channel to maintain data's integrity.

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	
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	Comment #32: The email address is provided by subscriber into the documents registration. The Certificate Manager verifies that the email is correct and is attached to his organization before sending to Registration Service. Registration service is a group of person of SG Trust Services. In technical process, only the subscriber can receive into the email declared on registration documents the install URL of his 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	No
Distributing generated private keys in PKCS#12 files	Not SSL
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	CRLs import without error 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.