Bugzilla ID: 527419
Bugzilla Summary: Add Secom Trust SHA256 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	SECOM Trust Systems Co., Ltd.
Website URL	http://www.secomtrust.net/
Organizational type	Commercial
Primary market / customer base	Japan
CA Contact Information	**CA Email Alias:** h-kamo@secom.co.jp, koi-takahashi@secom.co.jp An email alias is requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization. **CA Phone Number:** 81-3-5775-8674 **Title / Department**: Secure Service Department

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**
Certificate Name	Security Communication RootCA2 No CN; OU = Security Communication RootCA2; O = "SECOM Trust Systems CO.,LTD."
Cert summary / comments	Is this the SHA256 version of the "Security Communication RootCA1" (SHA1) root certificate that is currently in Mozilla/NSS?
The root CA certificate URL	https://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer
SHA-1 fingerprint	5F:3B:8C:F2:F8:10:B3:7D:78:B4:CE:EC:19:19:C3:73:34:B9:C7:74
Valid from	2009-05-28
Valid to	2029-05-28
Cert Version	3
Modulus length / key length	2048
Test Website	https://fmctest.secomtrust.net/
CRL URL	https://repository.secomtrust.net/SC-Root2/SCRoot2CRL.crl http://testrepository.secomtrust.net/subca6/fullcrl.crl (NextUpdate 1 month) CRL issuing frequency for subordinate end-entity certificates: 1 day Please provide the document url and page number where the CP/CPS states the CRL issuing frequency.

OCSP Responder URL	None
CA Hierarchy	Please explain and/or provide a diagram of the current and planned CA Hierarchy for this root.
Sub-CAs operated by 3rd parties	Does or will this root have any subordinate CAs that are operated by external third parties?
Cross-Signing	List any other root CAs that have issued cross-signing certificates for this root CA
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type DV, OV, and/or EV	DV? OV? EV? Within this root hierarchy… 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)	EV? If EV, please point me to the relevant EV CP/CPS documentation (URL and page numbers) of subscriber verification procedures for EV certs.
CP/CPS	Documents relating to this root: https://repository.secomtrust.net/SC-Root2/index.html CPS (Japanese): https://repository.secomtrust.net/SC-Root/SCRootCPS.pdf CP (Japanese): https://repository.secomtrust.net/SC-Root/SCRootCP1.pdf
AUDIT	Audit Type: WebTrust Readiness Audit Auditor: KPMG Auditor Website: http://www.kpmg.com Audit Document URL(s): https://cert.webtrust.org/SealFile?seal=975&file=pdf The above URL is the reports for our other root certificates. Regarding the "Security Communication RootCA2", it is not publicly accessible because of the readiness audit. We will give you the readiness audit report upon your request. Please attach the non-confidential portion of the readiness audit for this root to the bug report or provide a url. If EV, we'll need both the WebTrust CA and WebTrust EV.
Organization Identity Verification	Google Translations of SCRootCP1 – Please Correct. 3.2 Identification and authentication of the first 3.2.1 Method to prove possession of private key SECOM route operated by the CA certificate request was submitted by the applicant a certificate (Certificate Signing Request: following, "CSR" it) and signature verification to verify that the corresponding private key is signed with public key contained in it. In addition, CSR to check the fingerprint, to identify the owner of a public key. 3.2.2 Authentication of organization or organizations Applicant's certificate, the certificate when applying for a root CA must be operated out SECOM provides information on the following. Application for certificate issuance, Information, the real proof that the organization or organizations · CSR Such other routes operated by Secom

	Secom documents required by the CA is using the information above, make sure that there are no errors or missing information in the application. 3.2.3 Authentication of individual Operated Secom root CA will not issue certificates to individuals. 3.2.4 Validation of authority Secom root CA is operated by representatives of organizations or groups and certificate applicants, or employees who Osamu generation, that has the legal authority to apply for information about the organization or organizations Check. 4. Requirements for certificate life-cycle management 4.1 Certificate Application 4.1.1 The application can perform certificate Apply for issuance of certificates, representatives of organizations or groups to apply for issuance, can be performed by employees or agents. 4.1.2 Registration procedures and responsibilities Certificate applicant is operated Secom root CA has been notified in advance in accordance with procedures than to apply for the certificate. Certificate applicant is issued a certificate to apply Niatari, this CP, CPS, and other root CA and operated by SECOM to accept the contents of those documents was disclosed. Certificate applicant is operated Secom root CA must ensure that accurate information on what application. 4.2 Certificate Application Procedures 4.2.1 Identification and authentication procedures Secom root CA is operated, the applicant submits an application for a certificate of receipt of application documents and the authenticity of CSR, this CP "3.2 initial identification and authentication" check under. Acceptance or rejection of certificate applications 4.2.2 Secom root CA is operated in accordance with predetermined procedures for screening applicants for a certificate from the applicant to determine the affirmative or negative of the request for issuance of a certificate, a certificate to the applicant to notify the results. 4.2.3 Certificate Application Processing Time Secom root CA is operated, if you accept the request for issuance of a certificate from the applicant to issue certificates immediately. 4.3 Certificate 4.3.1 CA certificates issued during the processing procedures Secom root CA is operated, was submitted by the applicant's public key certificate for CSR, this CP "7.1 Certificate profile" according to content, operated by Secom root CA's private key using a signature to issue a certificate stating. 4.3.2 Notification of certificate issuance to subscriber Secom root CA is operated after the completion of an application for issuance of certificates received and stored in the external storage media such as floppy disks certificates issued, after sealing with a receipt and certificate applicants

	certificate sent to the applicant by mail or delivered personally or between. 4.4 confirm receipt of the certificate 4.4.1 confirmation of receipt of the certificate procedure Applicant's certificate to verify the contents of the certificate at the time was not considered a problem, the root CA must be operated by SECOM for sending the receipt. Secom root CA is operated to accept the certificate of completion and received a receipt at the time. However, if there are errors in the contents of the certificate, the applicant operated Secom root certificates to that effect without delay should contact the CA. Complaints about the contents of the certificate is sent from the date of the certificate must be made within 14 days. 4.4.2 Publication of the certificate Secom root CA is operated by a subordinate CA certificate not in principle the public and subscribers. 4.4.3 Notification of certificate issuing CA to other entities of Operated Secom root CA is not a notice of the issuance of certificates for other entities. 4.5 key pair and certificate usage 4.5.1 use of the subscriber's private key and certificate Operated by Secom root CA private key applications and possess a certificate issued by the subscriber, or service that is provided by Secom, a route operated by a contractual relationship with Secom Secom provides subscribers CA Applications are limited to services or products that are prescribed. Secom root CA certificate to operate is issued, it should not be used for any other purpose. 4.5.2 The purpose of the user's public key and certificate Users are familiar with this CPS and CP contents of Secom operated on the route have agreed to use the CA certificate, the root CA to be operated by Secom verify the authenticity of the certificate issued by not.
Domain Name 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 SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate *or* has been authorized by the domain registrant to act on the registrant's behalf; Please provide translations into English of the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber. Please also list the corresponding document(s) and section or page numbers containing the original text.
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;

	Please provide translations into English of the sections of the CP/CPS documents that describe the procedures for verifying that the email account associated with the email address in the cert is owned/controlled by the subscriber. Please also list the corresponding document(s) and section or page numbers containing the original text.
Identity of Code Signing Subscriber	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 certificates to be used for digitally signing code objects, the CA takes reasonable measures to verify that the entity submitting the certificate signing request is the same entity referenced in the certificate *or* has been authorized by the entity referenced in the certificate to act on that entity's behalf; Please provide translations into English of the sections of the CP/CPS documents that describe the identity verification procedures for code signing certs. Please also list the corresponding document(s) and section or page numbers containing the original text.
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 this root. For the ones that are applicable, please provide further information and translations into English of the CP/CPS where relevant. • Long-lived DV certificates o • Wildcard DV SSL certificates o • Delegation of Domain / Email validation to third parties o • Issuing end entity certificates directly from roots o • Allowing external entities to operate unconstrained subordinate CAs o • Distributing generated private keys in PKCS#12 files o • Certificates referencing hostnames or private IP addresses o • OCSP Responses signed by a certificate under a different root o • CRL with critical CIDP Extension o • Generic names for CAs o Name is not generic