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 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
Cert summary / comments	This is the SHA256 version of the "Security Communication RootCA1" (SHA1) root certificate that is currently in NSS. It will have separate intermediate CAs for signing certificates for SSL, email, and code signing.
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://scrootca2test.secomtrust.net
CRL URL	ARL: https://repository.secomtrust.net/SC-Root2/SCRoot2CRL.crl CRL Distribution Point in cert of test website: http://testrepository.secomtrust.net/subca6/fullcrl.crl CRL issuing frequency for subordinate end-entity certificates: 24 hours From SECOM CA Service Passport for Web SR 2.0 Certificate Policy (PfWSR2CA-CP.pdf), Section4.9.7: CRL is expired regardless of treatment, every 24 hours
OCSP Responder URL	None (Currently EV status is not shown in case OCSP fails, but shows the regular SSL UI.)

CA Hierarchy	CA Hierarchy Diagram for EV: https://bugzilla.mozilla.org/attachment.cgi?id=446676 This root certificate will sign the "Security Communication EV RootCA2" intermediate CA, which will sign the "SECOM Passport for Web EV CA2" intermediate CA, which will sign end-entity EV SSL certificates. This root will also have separate intermediate CAs for signing end-entity certificates for email (S/MIME) and code signing.
Sub-CAs operated by 3rd parties	None
Cross-Signing	None
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type DV, OV, and/or EV	OV, EV
EV policy OID(s)	1.2.392.200091.100.721.1
CP/CPS	Diagram showing relation of documents: https://bugzilla.mozilla.org/attachment.cgi?id=447053 Documents relating to this root: https://repository.secomtrust.net/SC-Root2/index.html Security Communication RootCA Certification Procedures for Operation (Japanese): https://repository.secomtrust.net/SC-Root/SCRootCPS.pdf Security Communication RootCA Subordinate CA Certificate Policy (Japanese): https://repository.secomtrust.net/SC-Root/SCRootCP1.pdf SECOM CA Service Passport for Web SR 2.0 Certificate Policy (Japanese): https://repo1.secomtrust.net/spcpp/pfw/pfwsr2ca/PfWSR2CA-CP.pdf SECOM Passport for Web EV Certificate Policy (Japanese): https://repo1.secomtrust.net/spcpp/pfw/pfwevca/PfWEVCA-CP.pdf SECOM Passport for Web EV Certificate Policy (copy-and-paste enabled): https://bugzilla.mozilla.org/attachment.cgi?id=449589 EV Verification Document: https://bugzilla.mozilla.org/attachment.cgi?id=451885 Comment #16: Please understand that the only sections for the verification of the organization and the domain owner are attached.
AUDIT	Audit Type: WebTrust CA Readiness Audit Auditor: KPMG Auditor Website: http://www.kpmg.com Audit Document URL(s): https://cert.webtrust.org/SealFile?seal=975&file=pdf (2009.06.08 – includes RootCA1) Readiness Audit: https://bugzilla.mozilla.org/attachment.cgi?id=447054 (2009.06.08 – RootCA2 Readiness) No WebTrust EV Audit yet. The EV intermediate issuing CA has not yet been constructed.

Organization Identity Verification	Translations from Security Communication RootCA Subordinate CA Certificate Policy (SCRootCP1) 3.2 Initial identification and authentication 3.2.1 Method to prove possession of private key Route CA operated by Secom verify the signature of the Certificate Signing Request: following, "CSR" submitted by the applicant and verify that the corresponding public key contained in it is signed with private key. In addition, check the fingerprint of the CSR to identify the owner of the public key. 3.2.2 Authentication of organization Applicant must submit the following when apply the certificate. - Application for certificate issuance - Information that shows the existence of the organization - CSR - Any other documents if required by Secom Secom use the information above and make sure that there are no errors or missing information in the application. 3.2.3 Authentication of individual Root CA operated by Secom does not issue certificates to individuals. 3.2.4 Validation of authority Secom validate the representatives, employees or agents of organizations or groups who have the legal authority to apply certificates. 4. Requirements for certificate life-cycle management 4.1 Certificate Application 4.1.1 The one who can apply certificate Application of issuance for certificates can be performed by representatives, employees or agents of organizations or groups. 4.1.2 Registration procedures and responsibilities Applicant applies for the certificate in accordance with procedures notified by Secom in advance. Applicant who applies for the certificate accepts CP, CPS, and other contents of those documents disclosed by Secom. Applicant must ensure the accuracy of information on that application. 4.2 Certificate Application Procedures 4.2.1 Identification and authentication procedures Secom validates the application documents submit by the applicant and authenticity of CSR conformed with this CP "3.2 initial identification and authentication". 4.2.2 Acceptance or rejection of certificate applications Secom notifies the applicant for the results whether accept or reject for the application after the validation in accordance with predetermined procedures. 4.2.3 Certificate Application Processing Time Secom issues the certificate immediately if the application is accepted.

	4.3 Issuance of certificate 4.3.1 Procedures to issue certificate by CA Secom issues the certificate by signing Secom root CA's private key to the applicant's public key certificate for CSR according to the content of CP "7.1 Certificate profile". 4.3.2 Notification of certificate issuance to subscriber Secom sends the certificate issued that is sealed with a receipt and stored in the external storage media such as floppy disks to the applicant by delivered personally or mail 4.4 Confirmation for receipt of the certificate 4.4.1 Confirmation procedure for receipt of the certificate Applicant must send the receipt to Secom at the timing verified the contents of the certificate. Secom realizes the completion of the procedure at the timing of get the receipt. However, if there are errors in the contents of the certificate, the applicant must contact Secom without delay. Complaints about the contents of the certificate must be made within 14days after the date the certificate was sent. 4.4.2 Publication of the certificate Secom root CA is not in principle the public the subordinate CA certificates. 4.4.3 Notification of certificate issuing by CA to other entities Secom root CA does not notify the issuance of certificates for other entities. 4.5 Usage of key pair and certificate 4.5.1 Usage of the subscriber's private key and certificate The usage of the certificates issued by Secom root CA and private keys possessed by applicants are limited to services provided by Secom or services provided by subscribers of Secom root CA that is contractual relationship with Secom. The certificates issued by Secom root CA should not be used for any other purpose. 4.5.2 Usage of the user's public key and certificate Users are familiar with CP and CPS and agree to use root CA and verify the authenticity of the certificate issued by Secom root CA.
Domain Name Ownership / Control EV	Translations of sections 3.2, 3.3 and 3.4 of PfWEVCA-CP (https://bugzilla.mozilla.org/attachment.cgi?id=449589) 3.2 Initial identification and authentication 3.2.1 Method to prove possession of private key It is proved that the applicant has the private key as follows. Certificate Signing Request, "CSR" submitted by the applicant and verify that the corresponding public key contained in it is signed with private key. In addition, check the fingerprint of the CSR to identify the owner of the public key. 3.2.2 Authentication of company Secom authorize the authentication of the applicant company as follows. By using the official documents from central or local government, database provided by QIIS or QGIS, and another ways that the equal level of authorization possible. 3.2.3 Authentication of individual

	Secom authorize the authentication of the applicant individual as follows. By using the official documents from central or local government, database provided by QIIS or QGIS, and another ways that the equal level of authorization possible. 3.2.4 Information of non verified certicate user Not described. 3.2.5 Confirmation of the authority to apply Secom confirm that the applicant has proper right to apply the certificate by the section 3.2 or 3.3 on this CP. In the case if the application is made by third party, we request to give us the letter of attorney. * The third party application means that other than the company using the host name described on common name of the certificate that is described on the section 3.1.1. 3.2.6 This CA is issued one-way cross signing certificate from Security Communiation EV RootCA1. 3.3 Identification and authentication at renewal application 3.3.1 Identification and authentication at usual renewal application It is same as 3.2. 3.3.2 Identification and authentication at renewal application after revocation No renewal for revoked certificate. The application is treated as new and it is same as 3.2. Translations of Secom Passport for Web EV service verification procedures that were attached to the bug. https://bugzilla.mozilla.org/attachment.cgi?id=451885 2.3 procedure3. Physical existence of the applicant The below is the procedures to verify the physical existence of the applicant. (1) Current address is same with the QIIS/ QGIS and the one on the application. QIIS/QGIS(EDINET(https://info.edinet.go.jp/EdiHtml/main.htm)) (2) If we cannot verify by (1), RA or operation manager visits the current address and verify the physical existence. (3) If we cannot verify by (1) or (2), we verify by lawyer opinion letter. We verify: (a) The address for the current physical existence on the letter. (b) The real existence of the lawyer who wrote the letter. 2.4 procedure 4. Domain/ CSR verification 4-1. The contents of (O) for CSR 4-1-1. Registered corporation We verify the (O) is same as the financial statements publicly available on the Web site. If the financial statements is not available, it is verified by QIIS or QGIS. If it is not verified by the above, it is verified by certificate of incorporation or lawyer opinion letter. And again, if it is not verified by the above, it should be roman alphabet of Hepburn system. For example, Secom CO.,LTD. => sekomu kabushikigaisya Wrong with the domain

	The certificate was issued with the same DN before except the case of renewal or reissue. For the above, we ask the applicant to remake the CSR and apply again. * For more detail, please refer to "4. Check for the content of CSR for supplementation". 4-1-2. Government ministries and agencies and organization in country/local public entity We verify the (O) is same as QIIS, QGIS and get the screen capture. If it is not verified by QIIS, QGIS, it should be roman alphabet of Hepburn system. For example, Yokohama city => Yokohamashi Government and municipal offices => Kankocho Wrong with the domain The certificate was issued with the same DN before except the case of renewal or reissue. For the above, we ask the applicant to remake the CSR and apply again. * For more detail, please refer to "4. Check for the content of CSR for supplementation". 4-1-3. University/ National and public high school We verify the (O) is same as QIIS, QGIS and get the screen capture. If it is not verified by QIIS, QGIS, it should be roman alphabet of Hepburn system. For example, Tokyo university => Tokyo daigaku Wrong with the domain The certificate was issued with the same DN before except the case of renewal or reissue. For the above, we ask the applicant to remake the CSR and apply again. * For more detail, please refer to "4. Check for the content of CSR for supplementation". 4-2 Verification of the domain owner By using Whois gateway(NIC domain reference function), we verify the applied company name on domain information (the contents included in CommonName) and the applicant (if the domain name use consent form is submitted, it is same as the domain owner). The two points to check for exclusive right to use. For example, the applied CN is "WWW.login.secom.co.jp" (1) Applied company or company that exists in parents/child relation with the applied company owns "secom.co.jp". (2) Applied company or company that exists in parents/child relation with the applied company owns "login.secom.co.jp". In order to check for parents/child relation, we use QIIS or QGIS(EDINET). If we cannot find it, we ask the applicant to change the owner as same as the applicant company name for WHOIS. If we cannot refer the owner at Whois gateway, ask the applicant for registration. JP domain: http://whois.jprs.jp/ COM, NET, ORG domain: http://www.networksolutions.com/cgi-bin/whois/whois Other than the above: http://www.uninett.no/navn/domreg.html

	4-2-1. For the domain owner is different from the applicant company In order to verify the exclusive ownership, we check either document below if the domain owner is third party. Domain name use consent form Lawyer opinion letter Points to be checked on the lawyer opinion letter is below. (1) It is described that the domain (secondary domain) is exclusively owned by the applicant company. The domain name is described at item #5 on the lawyer opinion letter. (2) The lawyer who wrote the lawyer opinion letter is really existing that is checked with 6. Check for the existence of the lawyer for supplementation.
Domain Name Ownership / Control non-EV	From SECOM: The procedure we verify of domain owner is same for EV and Non-EV SSL. The only difference is that no lawyer opinion letter is used for Non-EV SSL. See translation of section 4.2 of the verification procedures above.
Email Address Ownership / Control	Translations of sections 3.2, 3.3 and 3.4 of CP at the URL below. https://repo1.secomtrust.net/spcpp/pfm20pub/PfM20PUB-CP.pdf 3.2 Initial identification and authentication 3.2.1 Method to prove possession of private key Secom confirm that Certificate Signing Request submitted by the applicant and verify that the corresponding public key contained in it is signed with private key. In addition, check the fingerprint of the CSR to identify the owner of the public key. 3.2.2 Authentication of company Secom authorize the authentication of LRA or company as follows. By using the official documents from central or local government, database provided by QIIS or QGIS, and another ways that the equal level of authorization possible. In the case the official documents provided by central or local government, we request to give us Certificate of seal impression (issued within 3months) or equivalent as this. 3.2.3 Document to be submitted The documents provided to Secom is as follows. • The information described about the LRA or the company. • Another documents for verification required by Secom. If Secom judge the application is inappropriate after the verification, we return the all documents. We destroy the application form. 3.2.4 Authentication of applicant and certificate user Verification for applicant and certificate user is conducted by the method decided by LRA based on the operation standard.

	Translations of Mail Authentication Service Verification Procedure provided by SECOM 6. procedure4. Certificate information Verify for DN information Whether or not there is a mistake on DN information. - Not same for company name - Spelling mistake - Domain name mistake - The certificate was issued with the same DN before except the case of renewal or reissue. - Authentication by sending and receiving email. If it is not possible to send or receive the email, we verify the applied email address by making phone call or by another ways to the applicant company. 7. procedure5. Verification of the domain owner By using Whois gateway(NIC domain reference function), we verify the applied company name on domain information (the contents included in CommonName) and the applicant (if the domain name use consent form is submitted, it is same as the domain owner). JP domain: http://whois.jprs.jp/ COM, NET, ORG domain: http://www.networksolutions.com/cgi-bin/whois/whois Other than the above: http://www.uninett.no/navn/domreg.html 8. procedure6. Verification by phone call By making phone call to applicant company and make sure that the applicant belongs to the company and apply for the certificate.
Identity of Code Signing Subscriber	SECOM verifies the organization by QIIS or Certificate of the seal impression, and confirms the request of the certificate by making phone call to HRM of the organization. Possession of private key is confirmed as signing public key included in CSR by private key. It is described at section 3 “Identification and authentication” on CP.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  ○ SSL certs are OV
	• Wildcard DV SSL certificates
	  ○ SSL certs are OV
	• Delegation of Domain / Email validation to third parties
	  ○ Not applicable
	• Issuing end entity certificates directly from roots
	  ○ Not applicable.
	• Allowing external entities to operate unconstrained subordinate CAs
	  ○ Not applicable.

	• Distributing generated private keys in PKCS#12 files
	  ○ No.
	• Certificates referencing hostnames or private IP addresses
	  ○ None.
	• OCSP Responses signed by a certificate under a different root
	  ○ No.
	• CRL with critical CIDP Extension
	  ○ No.
	• Generic names for CAs
	  ○ Name is not generic