Bugzilla ID: 1096205
Bugzilla Summary: Enable EV for Security Communication RootCA2

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	SECOM Trust Systems Co., Ltd.
Website URL	http://www.secomtrust.net/
Organizational type	Commercial
Primark Market / Customer Base	Japan
Impact to Mozilla Users	SECOM is a Japanese commercial CA that provides SSL and client certificates for e-Government and participates in several projects for financial institutions to ensure the secured on-line transactions. SECOM provides information security services, including authentication and secure data center management services, as well as safety confirmation services, which assist companies in the event of a large-scale disaster.
Inclusion in other major browsers	Yes. Mozilla, Microsoft, Apple.
CA Primary Point of Contact (POC)	CA Email: h-kamo@secom.co.jp, koi-takahashi@secom.co.jp CA Phone Number: 81-3-5775-8674 Title / Department: Secure Service Department

Technical information about each root certificate

Certificate Name	Security Communication RootCA2

Certificate Issuer Field	OU = Security Communication RootCA2
	O = "SECOM Trust Systems CO.,LTD."
	C = JP

Certificate Summary	Requesting EV-treatment for root certificate that was included via Bugzilla Bug #527419.
Mozilla Applied Constraints	None
Root Cert URL	https://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer
SHA1 Fingerprint	5F:3B:8C:F2:F8:10:B3:7D:78:B4:CE:EC:19:19:C3:73:34:B9:C7:74
Valid From	2009-05-29
Valid To	2029-05-29
Certificate Version	3
Certificate Signature Algorithm	SHA-256
Signing key parameters	2048
Test Website URL (SSL)	Need URL to website whose EV SSL cert chains up to this root.
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 URL	OCSP URI in the AIA of end-entity certs Maximum expiration time of OCSP responses
EV Testing Results	https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	OV and EV
EV Policy OID(s)	1.2.392.200091.100.721.1
Non-sequential serial numbers and entropy in cert	http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html "9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: ... - all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number)."
Response to Recent CA Communication(s)	Done

CA Hierarchy information for each root certificate

CA Hierarchy	This root certificate has internally-operated subordinate CAs which sign end-entity certificates for SSL, EV SSL, email (S/MIME), and code signing. EV CA Hierarchy Diagram: https://bugzilla.mozilla.org/attachment.cgi?id=8519800 Intermediate CAs are available here: https://www.secomtrust.net/service/pfw/apply/sr/3_2.html https://www.secomtrust.net/service/pfw/apply/ev/3_2.html
Externally Operated SubCAs	Can this root have externally-operated subordinate CAs? Does it currently have externally-operated subordinate CAs?
Cross-Signing	List all other root certificates for which this root certificate has issued cross-signing certificates. List all other root certificates that have issued cross-signing certificates for this root certificate. If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.
Technical Constraints on Third-party Issuers	Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate

Verification Policies and Practices

Policy Documentation	Documents are in Japanese. Security Communication RootCA2 Repository: https://repository.secomtrust.net/SC-Root2/index.html Root CPS: https://repository.secomtrust.net/SC-Root/SCRootCPS.pdf SubCA CP: https://repository.secomtrust.net/SC-Root/SCRootCP1.pdf SECOM CA Service Passport for Web SR 2.0 CP: https://repo1.secomtrust.net/spcpp/pfw/pfwsr2ca/PfWSR2CA-CP.pdf SECOM Passport for Web EV CP: https://repo1.secomtrust.net/spcpp/pfw/pfwevca/PfWEVCA-CP.pdf Is this the old version of the document attached to the bug? SECOM Passport for EV CP: https://bugzilla.mozilla.org/attachment.cgi?id=8519807 Where is this on the SECOM website?
Audits	Audit Type: WebTrust for CA, BR, and EV Auditor: PricewaterhouseCoopers Audit Report: https://cert.webtrust.org/SealFile?seal=1717&file=pdf (2014.07.31) BR Readiness audit for “SECOM Passport for Web EV 2.0 CA”: https://bugzilla.mozilla.org/attachment.cgi?id=8519802 (2014.09.19)
Baseline Requirements (SSL)	Please carefully review: https://wiki.mozilla.org/CA:BaselineRequirements (also have your auditor carefully review this wiki page) The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3.
SSL Verification Procedures	Please provide translations into English of the portions of the CP/CPS having to do with domain verification for SSL certificates, as per #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices Also indicate which sections of the original documents the translations come from.
EV Organization Verification Procedures	Please provide translations into English of the portions of the CP/CPS having to do with Organization Verification Procedures for EV SSL certificates. Also indicate which sections of the original documents the translations come from.
EV SSL Verification Procedures	Please provide translations into English of the portions of the CP/CPS having to do with domain verification for EV SSL certificates. Also indicate which sections of the original documents the translations come from.
Email Address Verification Procedures	Please provide translations into English of the portions of the CP/CPS having to do with email address verification for S/MIME certificates, as per #4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices Also indicate which sections of the original documents the translations come from.
Code Signing Subscriber Verification Procedures	Please provide translations into English of the portions of the CP/CPS having to do with verification of the identity and authority of the code signing certificate subscriber, as per #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices Also indicate which sections of the original documents the translations come from.

	If you are requesting to enable the Code Signing Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Multi-factor Authentication	Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Network Security	Confirm that you have performed the actions listed in #7 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	See above
CA Hierarchy	See above
Audit Criteria	See above
Document Handling of IDNs in CP/CPS	???
Revocation of Compromised Certificates	??? See Baseline Requirements section 13.1.5
Verifying Domain Name Ownership	See above
Verifying Email Address Control	See above
Verifying Identity of Code Signing Certificate Subscriber	See above
DNS names go in SAN	???
Domain owned by a Natural Person	???
OCSP	See above

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

Long-lived DV certificates	What is the maximum validity of SSL certs? Both non-EV and EV…
Wildcard DV SSL certificates	Are Wildcard certs allowed?
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	See above
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	???

SHA-1 Certificates	???
Generic names for CAs	No. See above.
Lack of Communication With End Users	???
Backdating the notBefore date	???