Print this page

Mozilla - CA Program

Case Information

Case Number	00000055	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	SECOM Trust Systems Co. Ltd.	**Request Status**	Initial Request Received

Additional Case Information

Subject	Enable EV-treatement for Security Communication RootCA2 root certificate	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1096205

General information about CA's associated organization

Company Website	http://www.secomtrust.net/	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Primary Market / Customer Base	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.	**Verified?**	Verified
Impact to Mozilla Users	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.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	We allow to use IDNs in certificates, but we haven't addressed this issue in neither CP nor CPS. -- ***Please add this to the appropriate CP/CPS.*** As described in subsection 4.9.1 of CP of this root CA, we revoke a certificate with private keys that are known to be compromised, or for which verification of subscriber	**Verified?**	Need Clarification From CA

information is known to be invalid.

We use SAN, as well as CN, to store DNS names.

The CP of this root CA restricts our subscribers to be organizations or groups.

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	The maximum validity of SSL certs is 60 months. As described at the BR, we will issume maximum validity for 39 months after April 2015.. We do not delegate validation to any third parties with respect to this root CA. -- ***Please clarify. It sounds like you do allow for externally-operated subordinate CAs, which means that a third-party can issue certificates. Therefore, a third-party does the domain/email validation.*** We have been issueing and will be issueing TA, TSA EE certficates, but no EV SSL certificates. -- ***What does TA and TSA EE certificates mean?*** We allow our customers to operate a subordinate CAs, but not for EV SSL certificates. -- ***Where is it documented that externally-operated subCAs cannot issue EV certificates? How is that enforced?*** We have been distributing generated keys in PKCS#12 and will be doing the same things for TLS/SSL client certficates, but not for TLS/SSL server certificates. We do not issue certificates for neither hostnames nor private IP addresses. We do not issue certificates for internal domains. We do not issue SHA-1 certificates from this root CA.	**Verified?**	Need Clarification From CA

Root Case Record # 1

Root Case Information

Root Case No	R00000072	**Case Number**	00000055
Request Status	Initial Request Received	**Root Certificate Name**	Security Communication RootCA2

Additional Root Case Information

Subject	Enable EV-Treatment for Security Communication RootCA2 root certificate

Technical Information about Root Certificate

O From Issuer Field	SECOM Trust Systems CO.,LTD.	**Verified?**	Verified
OU From Issuer Field	Security Communication RootCA2	**Verified?**	Verified
Certificate Summary	Requesting EV-treatment for root certificate that was included via Bugzilla Bug #527419.	**Verified?**	Verified
Root Certificate Download URL	https://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer	**Verified?**	Verified
Valid From	2009 May 29	**Verified?**	Verified
Valid To	2029 May 29	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	Need URL to test website whose EV SSL cert chains up to this root.	**Verified?**	Need Response From CA
CRL URL(s)	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	**Verified?**	Verified
OCSP URL(s)	http://ev2.ocsp.secomtrust.net/	**Verified?**	Verified
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
EV Policy OID(s)	1.2.392.200091.100.721.1	**Verified?**	Verified
EV Tested	Need successful output of EV Test: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	**Verified?**	Need Response From CA
Root Stores Included In	Apple; Microsoft; Mozilla	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	5F:3B:8C:F2:F8:10:B3:7D:78:B4:CE:EC:19:19:C3:73:34:B9:C7:74	**Verified?**	Verified
SHA-256 Fingerprint	51:3B:2C:EC:B8:10:D4:CD:E5:DD:85:39:1A:DF:C6:C2:DD:60:D8:7B:B7:36:D2:B5:21:48:4A:A4:7A:0E:BE:F6	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	This root certificate has subordinate CAs which sign end-entity certificates for SSL, EV SSL, email (S/MIME), and code	**Verified?**	Verified

	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	This root has externally-operated subordinate CAs. QUESTIONS: Can externally-operated SubCAs issue SSL certs? Can externally-operated SubCAs issue EV certs? Please provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist	**Verified?**	Need Clarification From CA
Cross Signing	None.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	We impose no technical constraints on third-party issuers. Then all subordinate CAs have to be audited and disclosed as described in sections 8 through 10 of https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ Please explain how this policy is met.	**Verified?**	Need Clarification From CA

Verification Policies and Practices

Policy Documentation	Documents are in Japanese.	**Verified?**	Verified
CA Document Repository	https://repository.secomtrust.net/SC-Root2/index.html	**Verified?**	Verified
CP Doc Language	Japanese		
CP	https://bugzilla.mozilla.org/attachment.cgi?id=8519807	**Verified?**	Verified
CP Doc Language	Japanese		
CPS	https://repository.secomtrust.net/SC-Root/SCRootCPS.pdf	**Verified?**	Verified
Other Relevant Documents	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 EV CP: https://bugzilla.mozilla.org/attachment.cgi?id=8519807 The EV CP is Not yet available on SECOM website -- SECOM is waiting for browsers to enable EV-treatment before posting this on their website.	**Verified?**	Verified

Auditor Name	PricewaterhouseCoopers Aarata	**Verified?**	Verified
Auditor Website	http://www.pwc.com/jp/en/assurance/corporate/in...	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1717&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	7/31/2014	**Verified?**	Verified
BR Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8519802	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	9/19/2014	**Verified?**	Verified
EV Audit	https://cert.webtrust.org/SealFile?seal=1717&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	7/31/2014	**Verified?**	Verified
BR Commitment to Comply	Section 1.1 in EV CP. QUESTION: Where is the commitment to comply with the Baseline Requirements for non-EV SSL certificates? Mozilla process requires re-verification of the CP/CPS information for all trust bits enabled for this root.	**Verified?**	Need Clarification From CA
SSL Verification Procedures	Please provide translation into English of the relevant sections of the CP/CPS. "It is described at the CP section 3.2. Organization which uses the host name that is indicated on a common name of the certificate that described at the profile information as 3.1.1. The domain owners are verified at the JPNIC or Internic Database and if the domain owner is different from the organization the certificate issued, the permission letter should be presented. https://www.secomtrust.net/service/pfw/apply/ev/1_3.html"	**Verified?**	Need Clarification From CA
EV SSL Verification Procedures	Please provide translation into English of the relevant sections of the CP/CPS. "It is described at the CP section 3.2. Organization verification by QIIS(DUNS/TSR Database) or Certified copy of register and certificate of seal impression. Verify to make sure the website is provided by the organization applied and the telephone verification for the applicant. https://www.secomtrust.net/service/pfw/apply/ev/sts_1.html"	**Verified?**	Need Clarification From CA
Organization Verification Procedures	Please provide translation into English of the relevant sections of the CP/CPS.	**Verified?**	Need Clarification From CA

Email Address Verification Procedures	The Email trust bit is enable for this root certificate, so I have to re-verify that the relevant policy documentation clearly indicates how the email address is verified to be owned/controlled by the certificate subscriber. Please provide translation into English of the relevant sections of the CP/CPS.	**Verified?**	Need Clarification From CA
Code Signing Subscriber Verification Pro	The Code Signing trust bit is enable for this root certificate, so I have to re-verify that the relevant policy documentation clearly indicates how the certificate subscriber's identity and authority are verified. Please provide translation into English of the relevant sections of the CP/CPS.	**Verified?**	Need Clarification From CA
Multi-Factor Authentication	Although we haven't explicitly documented, we have been performing multi-factor authentication. Please clearly indicate how multi-factor authentication is acheived.	**Verified?**	Need Clarification From CA
Network Security	As section 6.7 of CPS of this root CA, we never connect this root CA to other systems.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://www.secomtrust.net/service/pfw/apply/sr/3_2.html https://www.secomtrust.net/service/pfw/apply/ev/3_2.html	**Verified?**	Verified