Print this page

Mozilla - CA Program

Case Information

Case Number	00000055	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	SECOM Trust Systems Co. Ltd.	**Request Status**	Ready for Public Discussion

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

CA Email Alias 1			
CA Email Alias 2			
Company Website	http://www.secomtrust.net/	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Japan	**Verified?**	Verified
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... Verify the registered hold of the domain or exclusive control of the domain name by using InterNIC and JPRS Whois database. Verify the applicant organization’s existence and identity by Qualified Independent Information Source (QIIS) or Certificate of the	**Verified?**	Verified

seal impression based on Japanese customs and practices. It is described at https://www.secomtrust.net/service/pfw/apply/ev/1_3.html
If the domain owner is different organization, the applicant organization must provide a domain use permission proof document sealed by the domain own organization.
The document is available at https://www.secomtrust.net/service/pfw/apply/ev/2_2.html

* 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 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. We do not delegate to allow for externally-operated subordinate CAs either. * We have been issuing and will be issuing Time Authority (TA), Timestamp Authority (TSA) EE certficates, but no EV SSL certificates. * We never provide signing for externally-operated subCAs issuing EV certificates. Regarding EV enablement, browser venders require WebTrust EV audit and without to get authorized, it is no way to issue EV certificates. * We have been distributing generated keys in PKCS#12 and will be doing the same things for TLS/SSL client certificates, 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?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	Security Communication RootCA2	**Root Case No**	R00000072
Request Status	Ready for Public Discussion	**Case Number**	00000055

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	https://pfwtest.secomtrust.net/	**Verified?**	Verified
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
Revocation Tested	http://certificate.revocationcheck.com/pfwtest.secomtrust.net No errors reported.	**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	// OU=Security Communication RootCA2,O="SECOM Trust Systems CO.,LTD.",C=JP "1.2.392.200091.100.721.1", "SECOM EV OID", SEC_OID_UNKNOWN, { 0x51, 0x3B, 0x2C, 0xEC, 0xB8, 0x10, 0xD4, 0xCD, 0xE5, 0xDD, 0x85, 0x39, 0x1A, 0xDF, 0xC6, 0xC2, 0xDD, 0x60, 0xD8, 0x7B, 0xB7, 0x36, 0xD2, 0xB5, 0x21, 0x48, 0x4A, 0xA4, 0x7A, 0x0E, 0xBE, 0xF6 }, "MF0xCzAJBgNVBAYTAkpQMSUwIwYDVQQKExxTRUNPTSBUcnVzdCBTeXN0ZW1zIENP" "LixMVEQuMScwJQYDVQQLEx5TZWN1cml0eSBDb21tdW5pY2F0aW9uIFJvb3RDQTI=" "", "AA==", Success!	**Verified?**	Verified
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 signing. 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 There is only one (internally-operated) subordinate CA that can issue EV certs, namely "SECOM Passport for Web EV 2.0 CA". Externally-operated subCAs are not allowed to issue EV certs.	**Verified?**	Verified
Externally Operated SubCAs	There is currently one externally-operated subCA, Fuji Xerox (https://bugzilla.mozilla.org/show_bug.cgi?id=1015772). SECOM plans to migrate this subCA to be internally-operated by SECOM and be included in SECOM's policy documentation and audit.	**Verified?**	Verified
Cross Signing	None.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	We impose no technical constraints on third-party issuers.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in Japanese. Translations of some sections attached to bug: https://bug1096205.bugzilla.mozilla.org/attachment.cgi?id=8573613	**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 non-EV SSL CP: https://repo1.secomtrust.net/spcpp/pfw/pfwsr2ca/PfWSR2CA-CP.pdf	**Verified?**	Verified

	EV SSL 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.		
Auditor Name	PricewaterhouseCoopers Aarata	**Verified?**	Verified
Auditor Website	http://www.pwc.com/jp/en/assurance /corporate/index.jhtml	**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. and Sectioon 1.1 in the non-EV SSL CP	**Verified?**	Verified
SSL Verification Procedures	https://www.secomtrust.net/service /pfw/apply/ev/1_3.html Verify the organization by QIIS or Certificate of the seal impression, and confirm the request of the certificate by making phone call to HRM of the organization. The procedure that SECOM follows to verify the domain owner is the same for EV and non-EV SSL certificates. The only difference is that no lawyer opinion letter is used for Non-EV SSL. Translations from section 4-2 of SECOM's Verification Document describe the process by which Whois is used to verify that the domain owner is the same as the certificate subscriber company name. See translations of some sections attached to bug: https://bug1096205.bugzilla.mozilla.org /attachment.cgi?id=8573613	**Verified?**	Verified
EV SSL Verification Procedures	See translations of some sections of EV CP attached to bug. https://bug1096205.bugzilla.mozilla.org /attachment.cgi?id=8573613 https://www.secomtrust.net/service /pfw/apply/ev/1_3.html check whether you are the owner of the	**Verified?**	Verified

domain.
If it ends with ".JP" - JPRS WHOIS (Japan Registry Services Co., Ltd.)
Other - InterNIC Whois Gateway (Network Solutions, Inc.)
And if it is in the old organization information, if there is a mistake in the registration information of the domain, please change to the correct information contact the domain management company.
If it is set the domain information in private, please publish the domain information.

https://www.secomtrust.net/service/pfw/apply/ev/sts_1.html
1. site content / operator confirmation
In SECOM Trust Systems, and because of the certificate to prove the existence of the web site, I will check and review
- The presence of the web site
- The existence of the organization that operates the web site
- Requesting organization information, certificate issuance destination information (CSR information) and match of the organization that operates the web site
2. Confirmation of application information / domain information / trade name
Confirmation of domain information
I'll make sure the organization that owns the domain.
If a third party (other than the applicant organization) owns the domain, we will submit the documents in order to confirm or being used consent with respect to the use of the domain. In addition, I will check the existence of the organization.

CP section 3.2: Verify the organization by QIIS or Certificate of the seal impression, and confirm the request of the certificate by making phone call to HRM of the organization.
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.

Organization Verification Procedures

See translations of some sections of CP attached to bug: https://bug1096205.bugzilla.mozilla.org/attachment.cgi?id=8573613

See online application process, starting here: https://www.secomtrust.net/service/pfw/apply/ev/1_1.html

https://www.secomtrust.net/service/pfw/apply/ev/sts_1.html
2. Confirmation of application information / domain information / trade name
Input information, I will check the submitted documents. ...
Establishment of less than three years organization
In legal entity of less than founded three years, if there is no company registration of Tokyo Shoko Research (below TSR)

Verified? Verified

	because of the organization confirmation, we will submit a lawyer written opinion. ... I'll make sure the organization that owns the domain. ... I will check the existence of the organization. Confirmation of trade name The English trade name to be registered in the CSR information, you can check any of the following. ... 3. Telephone confirmation (Application of intention confirmation / enrollment confirmation) Telephone number has been registered in the TSR of corporate information, or make the phone contact than 104 guidance number. - Confirmation of the applicant's and enrolled and officers to "HR of application organization" - Check the contents sign up for "registered representative" - Check your application approved by the "applicant"		
Email Address Verification Procedures	See translations attached to bug. ranslations 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.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	See translations of some sections of CP attached to bug: https://bug1096205.bugzilla.mozilla.org/attachment.cgi?id=8573613	**Verified?**	Verified
Multi-Factor Authentication	Although we haven't explicitly documented, we have been performing multi-factor authentication.	**Verified?**	Verified
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