Print this page

Mozilla - CA Program

Case Information

Case Number	00000084	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	SECOM Trust Systems Co. Ltd.	**Request Status**	Initial Request Received

Additional Case Information

Subject	Add two new root certificates	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1313982

General information about CA's associated organization

CA Email Alias 1	h-kamo@secom.co.jp		
CA Email Alias 2			
Company Website	http://www.secomtrust.net/english/outline.html	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Japan	**Verified?**	Verified
Primary Market / Customer Base	Japan	**Verified?**	Verified
Impact to Mozilla Users	base on the geographic focus, it impacts mozilla user in japan	**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	1. NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices 1) Publicly Available CP and CPS: CP https://sr4v.secomtrust.net/secom/SecomCP.docx CPS https://sr4v.secomtrust.net/secom/SecomCPS.docx 2) CA Hierarchy: (please provide which sections in CP/CPS) 3) Audit Criteria: WebTrust audit report is available at: https://cert.webtrust.org/SealFile?seal=2105&file=pdf 4) Document Handling of IDNs in CP/CPS: CA uses Japanese HIRAGANA,	**Verified?**	Need Clarification From CA

KATAKANA, KANZI as well as ASCII alpha numeric characters, which are used very often in Japanese language that their customers use.
CA authenticates the identity of domains based on investigations conducted or databases owned by third parties such as WHOIS registry service that SECOM Trust Systems trusts, and other methods determined to be equally trustworthy by the Certification Services Improvement Committee.
5) Revocation of Compromised Certificates: CA revokes a certificate in the event of the followings:
- The reliability of the certificate may have been lost due to reasons such as the theft, loss, unauthorized disclosure or unauthorized use of the relevant private key.
- The relevant private key has been or may be compromised, resulting in loss of confidentiality.
6) Verifying Domain Name Ownership: CA authenticates the identity of domains based on investigations conducted or databases owned by third parties such as WHOIS registry service that SECOM Trust Systems trusts, and other methods determined to be equally trustworthy by the Certification Services Improvement Committee.
7) Verifying Email Address Control: For a certificate to be used for digitally signing and/or encrypting email messages, CA takes measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate.
8) Verifying Identity of Code Signing Certificate Subscriber: CA authenticates the identity of organizations based on official documents issued by national and municipal governments, investigations conducted or databases owned by third parties that SECOM Trust Systems trusts, and other methods determined to be equally trustworthy by the Certification Services Improvement Committee.
9) DNS names go in SAN: CA uses CN as well as SAN for DNS names.
10) Domain owned by a Natural Person: For SSL/TLS server certificates, CA accept subscription application only from organizations and no natural persons.
11) OCSP: For OCSP services for end-entity certificates, CA all request subordinate CAs to update OCSP statuses at least every four days, and request OCSP responses from subordinates CAs to have a maximum expiration time of ten days.
12) Network Security Controls: A CA system is not connected to other internal or external systems. The repository system is protected from unauthorized access by such means as fire walls and intrusion detection systems.

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	2. NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices 1) Long-lived DV certificates: CA issues 24months certificates. Upon renewal, each certificates are verify that all of the information that is included in SSL certificates remains current and correct. 2) Wildcard DV SSL certificates: Currently, wildcard DV SSL certificates are issued, and CA will take consideration to identify to validate the organizaion. 3) Email Address Prefixes for DV Certs: Email addresses described acceptable are used for verification. 4) Delegation of Domain / Email validation to third parties: No delegation of domain/email validation to third parties. 5) Issuing end entity certificates directly from roots: No issuing end entity certificates directly from roots. 6) Allowing external entities to operate subordinate CAs: No external entities to operate subordinate CAs. 7) Distributing generated private keys in PKCS#12 files: No Distributing generated private keys in PKCS#12 files. 8) Certificates referencing hostnames or private IP addresses: CA does not issue certificates referencing hostnames or private IP addresses. 9) Issuing SSL Certificates for Internal Domains: CA does not issue certificates for internal domains.	**Verified?**	Need Clarification From CA

10) OCSP Responses signed by a certificate under a different root: CA does not have the environment such as OCSP Responses signed by a certificate under a different root.
11) SHA-1 Certificates: CA does not issue and does not have SHA-1 certificates.
12) Generic names for CAs: No, CA incorporate an organizational name Secom (Security Communication) for our names for CAs.
13) Lack of Communication With End Users: CA operates a 24x7 Helpdesk support center.
14) Backdating the notBefore date: CA does not issue certificates with Backdating the notBefore date.

Root Case Record # 1

Root Case Information

Root Certificate Name	Security Communication RootCA3	**Root Case No**	R00000125
Request Status	Information Verification In Process	**Case Number**	00000084

Certificate Data

Certificate Issuer Common Name	Security Communication RootCA3
O From Issuer Field	SECOM Trust Systems CO.,LTD.
OU From Issuer Field	
Valid From	2016 Jun 16
Valid To	2038 Jan 18
Certificate Serial Number	00e17c3740fd1bfe67
Subject	CN=Security Communication RootCA3, OU=null, O=SECOM Trust Systems CO.,LTD., C=JP
Signature Hash Algorithm	sha384WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	C3:03:C8:22:74:92:E5:61:A2:9C:5F:79:91:2B:1E:44:13:91:30:3A
SHA-256 Fingerprint	24:A5:5C:2A:B0:51:44:2D:06:17:76:65:41:23:9A:4A:D0:32:D7:C5:51:75:AA:34:FF:DE:2F:BC:4F:5C:52:94
Certificate Fingerprint	07:3B:A6:90:09:66:50:29:D9:FC:C2:41:33:33:EB:FD:5C:B7:D2:4D:85:96:3B:42:3A:3A:B0:ED:D4:ED:7C:E5
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	Root certificate, Security Communication RootCA3 is operated by SECOM Trust Systems Co., Ltd. (hereinafter "SECOM").	**Verified?**	Verified
Root Certificate Download URL	https://repository.secomtrust.net/SC-Root3/SCRoot3ca.cer	**Verified?**	Verified
CRL URL(s)	https://repository.secomtrust.net/SC-Root3/SCRoot3CRL.crl	**Verified?**	Verified
OCSP URL(s)	http://scrootca3.ocsp.secomtrust.net/	**Verified?**	Verified
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)		**Verified?**	Not Applicable
Root Stores	Microsoft	**Verified?**	Verified

Included In			
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs. https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551	**Verified?**	Need Response From CA

Test Websites or Example Cert

Test Website - Valid	https://sr4v.secomtrust.net/	**Verified?**	Verified
Test Website - Expired	https://sr4e.secomtrust.net/		
Test Website - Revoked	https://sr4r.secomtrust.net/		
Example Cert			
Test Notes			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	No errors	**Verified?**	Verified
CA/Browser Forum Lint Test	Certificate not found	**Verified?**	Verified
Test Website Lint Test	Test not currently available.	**Verified?**	Not Applicable
EV Tested	NO EV request	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. - List and/or describe all of the subordinate CAs that are signed by this root. - Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on. - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements	**Verified?**	Need Response From CA
Externally Operated SubCAs	NEED: - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist,https://wiki.mozilla.org/CA:SubordinateCA_checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.	**Verified?**	Need Response From CA
Cross Signing	NEED: - 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.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of version 1.3 of the CA/Browser Forum's Baseline Requirements - https://www.mozilla.org/en-US/about/governance/policies/security-	**Verified?**	Need Response From CA

group/certs/policy/inclusion/
-
https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions

Verification Policies and Practices

Policy Documentation	https://repository.secomtrust.net/SC-Root/SCRootCP1.pdf	**Verified?**	Verified
CA Document Repository	https://repository.secomtrust.net/SC-Root/SCRootCPS.pdf	**Verified?**	Verified
CP Doc Language	English		
CP	https://sr4v.secomtrust.net/secom/SecomCP.docx	**Verified?**	Verified
CP Doc Language	English		
CPS	https://sr4v.secomtrust.net/secom/SecomCPS.docx	**Verified?**	Verified
Other Relevant Documents	N/A	**Verified?**	Not Applicable
Auditor Name	Pricewaterhouse Coopers Aarata LLC	**Verified?**	Verified
Auditor Website	http://www.pwc.com/jp/en/assurance.html	**Verified?**	Verified
Auditor Qualifications	https://cert.webtrust.org/SealFile?seal=2105&file=pdf	**Verified?**	Verified
Standard Audit	NEED: for all root inclusion/change requests. Reference section 2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	N/A	**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. As per section 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference the section of the CA/Browser Forum's Baseline Requirements (BR) that lists the ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. The CA's CP/CPS must specify which of those options the CA uses, and must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the	**Verified?**	Need Response From CA

	domain name(s) to be included in the certificate. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership		
EV SSL Verification Procedures	No EV request	**Verified?**	Not Applicable
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert. As per section 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED CA response (and corresponding CP/CPS sections/text) to section 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	NEED CA response (and corresponding CP/CPS sections/text) to section 7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA

Root Case Record # 2

Root Case Information

Root Certificate Name	Security Communication ECC RootCA1	**Root Case No**	R00000126
Request Status	Initial Request Received	**Case Number**	00000084

Certificate Data

Certificate Issuer Common Name	Security Communication ECC RootCA1
O From Issuer Field	SECOM Trust Systems CO.,LTD.
OU From Issuer Field	
Valid From	2016 Jun 16
Valid To	2038 Jan 18
Certificate Serial Number	00d65d9bb378812eeb
Subject	CN=Security Communication ECC RootCA1, OU=null, O=SECOM Trust Systems CO.,LTD., C=JP
Signature Hash Algorithm	ecdsaWithSHA384
Public Key Algorithm	EC secp384r1
SHA-1 Fingerprint	B8:0E:26:A9:BF:D2:B2:3B:C0:EF:46:C9:BA:C7:BB:F6:1D:0D:41:41
SHA-256 Fingerprint	E7:4F:BD:A5:5B:D5:64:C4:73:A3:6B:44:1A:A7:99:C8:A6:8E:07:74:40:E8:28:8B:9F:A1:E5:0E:4B:BA:CA:11
Certificate Fingerprint	F7:43:46:8A:C3:9C:FF:6B:E0:02:74:60:13:19:C0:11:05:75:16:50:97:3D:15:1F:DB:E4:AB:26:38:4E:A6:70
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	Root certificate, Security Communication ECC RootCA1 is operated by SECOM Trust Systems Co., Ltd. (hereinafter "SECOM").	**Verified?**	Verified
Root Certificate Download URL	https://repository.secomtrust.net/SC-ECC-Root1/SCECCRoot1ca.cer	**Verified?**	Verified
CRL URL(s)	https://repository.secomtrust.net/SC-ECC-Root1/SCECCRoot1CRL.crl	**Verified?**	Verified
OCSP URL(s)	http://sceccrootca1.ocsp.secomtrust.net/	**Verified?**	Verified
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	N/A	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs. https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551	**Verified?**	Need Response From CA

Test Websites or Example Cert

Test Website - Valid	https://sr5v.secomtrust.net/	**Verified?**	Verified
Test Website - Expired	https://sr5e.secomtrust.net/		
Test Website - Revoked	https://sr5r.secomtrust.net/		
Example Cert			
Test Notes			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	No errors	**Verified?**	Verified
CA/Browser Forum Lint Test	Certificate not found.	**Verified?**	Verified
Test Website Lint Test	Test not currently available.	**Verified?**	Not Applicable
EV Tested	No EV request	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. - List and/or describe all of the subordinate CAs that are signed by this root. - Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on. - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements	**Verified?**	Need Response From CA
Externally Operated	NEED: - If this root has any subordinate CA certificates that are operated by external	**Verified?**	Need Response From CA

SubCAs	third parties, then provide the information listed in the Subordinate CA Checklist,https://wiki.mozilla.org/CA:SubordinateCA_checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.		
Cross Signing	NEED: - 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.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of version 1.3 of the CA/Browser Forum's Baseline Requirements - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ - https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	https://repository.secomtrust.net/SC-Root/SCRootCP1.pdf	**Verified?**	Need Clarification From CA
CA Document Repository	https://repository.secomtrust.net/SC-Root/SCRootCPS.pdf	**Verified?**	Need Clarification From CA
CP Doc Language	English		
CP	https://sr4v.secomtrust.net/secom/SecomCP.docx	**Verified?**	Verified
CP Doc Language	English		
CPS	https://sr4v.secomtrust.net/secom/SecomCPS.docx	**Verified?**	Verified
Other Relevant Documents	N/A	**Verified?**	Not Applicable
Auditor Name	Pricewaterhouse Coopers Aarata LLC.	**Verified?**	Verified
Auditor Website	http://www.pwc.com/jp/en/assurance.html	**Verified?**	Verified
Auditor Qualifications	https://cert.webtrust.org/SealFile?seal=2105&file=pdf	**Verified?**	Verified
Standard Audit	NEED: for all root inclusion/change requests. Reference section 2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Standard Audit Type		**Verified?**	Need Response From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA

EV Audit	N/A	**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. As per section 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference the section of the CA/Browser Forum's Baseline Requirements (BR) that lists the ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. The CA's CP/CPS must specify which of those options the CA uses, and must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership	**Verified?**	Need Response From CA
EV SSL Verification Procedures	No EV request	**Verified?**	Not Applicable
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert. As per section 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED CA response (and corresponding CP/CPS sections/text) to section 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	NEED CA response (and corresponding CP/CPS sections/text) to section 7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA