Bugzilla ID: 394419
Bugzilla Summary: Add secomtrust EV Root CA

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.

General Information	Data
CA Name	SECOM Trust Systems CO., LTD.
Website URL (English version)	http://www.secomtrust.net/
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	Commercial
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	Japan

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data	Status / Notes
Certificate Name	Security Communication EV RootCA1	COMPLETE
Cert summary / comments	This CA is a newly constructed root that needs to be added to Firefox. There is currently a non-EV CA called "Security Communication RootCA1" in Firefox. The CA hierarchy diagram (https://bugzilla.mozilla.org/attachment.cgi?id=298919)	COMPLETE
The root CA certificate URL Download into FireFox and verify	https://repository.secomtrust.net/EV-Root1/EVRoot1ca.cer	COMPLETE
SHA-1 fingerprint.	FE:B8:C4:32:DC:F9:76:9A:CE:AE:3D:D8:90:8F:FD:28:86	COMPLETE

	:65:64:7D	
Valid from	6/6/2007	COMPLETE
Valid to	6/6/2037	COMPLETE
Cert Version	3	COMPLETE
Modulus length / key length	2048	COMPLETE
CRL • URL • update frequency for end-entity certificates	CRL HTTP URL: http://repository.secomtrust.net/EV-Root1/EVRoot1CRL.crl "CP of SECOM Passport for Web EV CA, written in Japanese, states that it is 24H the frequency at which the CRLs for end-entity certificates must be updated." "Our CP in Japanese also states that it is 96H the lifetime between ThisUpdate and NextUpdate."	COMPLETE
OCSP (if applicable) • OCSP Responder URL • Max time until OCSP responders updated to reflect end-entity revocation EV Guidelines section 26(a): "OCSP responses from this service MUST have a maximum expiration time of ten days."	None	COMPLETE
List or description of subordinate CAs 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: 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.) For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant	https://bugzilla.mozilla.org/attachment.cgi?id=298919 Security Communication Root CA1 -> Security Communication EV Root CA 1 -> SECOM Passport for Web EV CA -> EV SSL Certificate	COMPLETE

CPS, and that any audit covers them as well as the root.		
For subordinate CAs operated by third parties, if any: General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which those subordinates are authorized, controlled, and audited. (For example, contractual arrangements should require third-party subordinates to operate in accordance with some CPS/CP. Technical arrangements might include name constraints, not allowing them to create their own subordinates, etc.)	"No. There are no CAs issued from the Security Communication EV Root CA1 that are controlled by third parties. We control the one and the only one CA issued from it."	COMPLETE
List any other root CAs that have issued cross-signing certificates for this root CA	SECOM Passport for Web EV CA is cross-signed by this root and by Secuirty Communication Root CA 1. "One of our root CAs, Security Communication Root CA1, has issued cross-signing certificate for Security Communication EV Root CA1. On the other hand, SECOM Passport for Web EV CA is not a root CA , but a subordinate CA signed by EV Root CA."	COMPLETE
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Websites Comment #18: Security Communication EV RootCA1 certificate needs to be marked for SSL use only at present, it does not need to be marked for another use. Our CPS/CP for Security Communication EV RootCA1 describes that the certificates use for server authentication and encription of data on the internet.	COMPLETE – only websites for now.
If SSL certificates are issued within the hierarchy rooted at this root CA certificate:	EV	COMPLETE

• Whether or not the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. (This is commonly referred to as a DV certificate.) • Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber. (This is commonly referred to as an OV certificate.) • Whether verification of the certificate subscriber conforms to the Extended Validation Certificate Guidelines issued by the CAB Forum. (This is commonly referred to as an EV certificate.)		
If EV certificates are issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.	1.2.392.200091.100.721.1	COMPLETE
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. • For SSL certificates this should also include URLs of one or more web servers using the certificate(s). • There should be at least one example certificate for each of the major types of certificates issued, e.g., email vs. SSL vs. code signing, or EV vs. OS vs. DV. • Note: mainly interested in SSL, so OK if no email example.	URL of website using certificate chained to this root (if applying for SSL): https://repo2.secomtrust.net/ev.gif	COMPLETE
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	https://repository.secomtrust.net/EV-Root1/ https://repository.secomtrust.net/EV-Root1/EVRoot1CPS.pdf From Hisashi Kamo: This information is documented on our homepage. In order to apply EV SSL certificate, the applicant read this and he must agree with this verification process. Regarding domain verification, we check with WHOIS database.	COMPLETE

	Based on the information from WHOIS database, we make a phone call to the contact of the domain holder. In the case where applicant is not the registered holder of the domain name, we verify applicant's exclusive right to use the domain name. We obtain positive confirmation from the registered domain holder by the form of "Domain usage consent form" that applicant has been granted the exclusive right to use the domain name. And then, making a phone call to the contact of the domain holder as the same procedures as the applicant is registered holder of the domain name.	
AUDIT: The published document(s) relating to independent audit(s) of the root CA and any CAs within the hierarchy rooted at the root. (For example, for WebTrust for CAs audits this would be the "audit report and management assertions" document available from the webtrust.org site or elsewhere.)	KPMG http://www.kpmg.com/ http://people.mozilla.com/~gen/secomtrust/SECOM-WTEV-Report.pdf Audit confirmed with Mark Lundin of KPMG mlundin@kpmg.com	COMPLETE AUDIT ISSUE: WTEV criteria requires backgroun employees. SECOM does not do background check Japanese customs. From Mark Lundin of KPMG: Regarding background checks, some jurisdictions su have legal limitations on what checks can be perfor The EV Guidelines contemplate this in section 29(2 states that certain checks shall be performed "where the jurisdiction where the person will be employed." We felt it was important to disclose the checks that performed in our report along with an explanation o circumstances in management's assertion. From Hisashi Kamo: As Mark-san mentioned on the email, some jurisdic Japan have legal limitations on what checks can be The EV Guidelines contemplate this in section 29(2 states that certain checks shall be performed "where

		the jurisdiction where the person will be employed" We believe this is what Microsoft be able to bridge they made arrangement of EV SSL for us.

Review CPS sections dealing with subscriber verification

- Verify domain check for SSL
    - Complete – see details above.
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - not applicable
- Verify identity info in code signing certs is that of subscriber
    - not applicable
- Make sure it's clear which checks are done for which context (cert usage)

Flag Problematic Practices

- Long-Lived Domain-Validated SSL certs
    - "We do not have such above certs at this point."
- Wildcard DV SSL certs
    - "We do not have such above certs at this point."
- Issuing end entity certs directly from root rather than using an offline root and issuing certs through a subordinate CA
    - "We do not have such above certs at this point."
- Allowing external entities to operate subordinate CAs
    - "We do not have such above certs at this point."

Verify Audits

- Validate contact info in report, call to verify that they did indeed issue this report.
    - COMPLETE
- For EV CA's, verify current WebTrust EV Audit done.
    - COMPLETE
- Review Audit to flag any issues noted in the report
    - ISSUE with background check process: SECOM doesn't do background checks of employees, but WTEV criteria requires this. From Hisashi Kamo: The EV Guidelines contemplate this in section 29(2) where it states that certain checks shall be performed "where allowed by the jurisdiction where the person will be employed". We believe this is what Microsoft be able to bridge this gap and they made arrangement of EV SSL for us.