Bugzilla ID: 496863
Bugzilla Summary: Add JCSI SecureSign RootCA11 root certificate

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, as per http://wiki.mozilla.org/CA:Information_checklist.

General Information	**Data**
CA Name	Japan Certification Services, Inc. (JCSI)
Website URL	http://www.jcsinc.co.jp/english/index.html
Organizational type	Public Commercial CA
Primary market / customer base	JCSI is a commercial CA whose primary market is Japan. Some of the relying parties are outside Japan, such as US, Canada, European countries, and Asia.

Info Needed	**Data**
Certificate Name	SecureSign RootCA11
Cert summary / comments	This root has one internally-operated subordinate CA for issuing SSL certificates to the public. In the future, JCSI plans to add other internally-operated subordinate CAs for S/MIME, Time Stamping, and other certificate types.
The root CA certificate URL	https://www2.jcsinc.co.jp/repository/certs/SSAD-rca.der
SHA-1 fingerprint.	3B:C4:9F:48:F8:F3:73:A0:9C:1E:BD:F8:5B:B1:C3:65:C7:D8:11:B3
Valid from	4/7/2009
Valid to	4/7/2029
Cert Version	3
Modulus length / key length	2048
Test Website(s)	https://ssad0406_2.jcsinc.co.jp/
CRL URL	Root CA primary CRLDP: http://ssignadcrl01.jcsinc.co.jp/repository/crl/rca.crl Root CA secondary CRLDP: http://ssignadcrl02.jcsinc.co.jp/repository/crl/rca.crl Subordinate CA primary CRLDP: http://ssignadcrl01.jcsinc.co.jp/repository/crl/sca1.crl Subordinate CA secondary CRLDP: http://ssignadcrl02.jcsinc.co.jp/repository/crl/sca1.crl nextUpdate for the URL for end-entity certs is 36 hours.
OCSP Responder URL	Not applicable
List or description of subordinate CAs operated by the CA organization associated with the root CA.	The SecureSign RootCA11 root has one internally-operated subordinate CA named SecureSign Public CA11, cert of which can be downloaded from: https://www2.jcsinc.co.jp/repository/certs/SSAD-sca1.der Currently there is no other internally operated subordinate CA's for this root. Additional subordinate CA's are under planning for S/MIME, Time Stamp Authority and other certificate types.

Subordinate CAs operated by third parties	None Currently there is no plan for this root to have subordinate CA's that are operated by external third parties.
List any other root CAs that have issued cross-signing certificates for this root CA	None Currently there is no plan for this root to cross certify, or to be cross certified by, any other root CA's.
Requested Trust Bits • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites (SSL/TLS)
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	OV JCSI performs identity/organization verification (OV) for SSL server certificates. The customer's ownership/control of the FQDN, and the existence and the identity of the organization, whose name and address are included in the certificate, are verified.
EV policy OID(s)	Not EV
CP/CPS	Repository: http://www.jcsinc.co.jp/english/repository/index.html CP/CPS in English: https://www2.jcsinc.co.jp/repository/SSAD-CPS-en.pdf The service under SecureSign RootCA11 root is governed by the CPS above. There are other CPS's listed in the web site for currently operated other services, whose root is not requested for the inclusion to Mozilla software.
AUDIT	Audit Type: WebTrust for CA Auditor: Ernst & Young ShinNihon LLC Audit Report and Management's Assertions: https://cert.webtrust.org/SealFile?seal=908&file=pdf (5.15.2009)

Review CPS sections dealing with subscriber verification
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify the domain referenced in an SSL cert is owned/controlled by the subscriber. In addition to verification of subscriber's legal identity.
    - CPS section 3: "In this sequence of steps, JCSI (i.e., the RAO) verifies and authenticates Web site identity. JCSI defines the verification and authentication of Web site identity as follows:
        - A check to confirm that the certificate application manager is qualified to manage the relevant Web site
        - A check to confirm that the certificate applicant (customer) is authenticated by the certificate application manager
        - A check to verify that the items (registration information on the certificate application) to be reflected in the certificate being applied for represent an authentic Web site (such as confirming the existence of the subscriber's organization, DNS name and identification of the owner)
        - A check to verify the correspondence between registration information on the certificate application described in the application form and information in the certificate signing request (CSR) and so on
- 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 requesting email trust bit.
- Verify identity info in code signing certs is that of subscriber
    - Not requesting code signing trust bit.

Flag Problematic Practices
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
    - SSL certs are OV
    - According to CPS: Subscriber Web server certificates are valid for 1 year
    - The CPS mentions long-term certs… Subscriber Long-term certificates for limited Time Stamp Authority and other type of certificates such as S/MIME are currently issued from under the other root, governed by another CPS. The migration of them to the SecureSign RootCA11 root is under planning.
- Wildcard DV SSL certificates
    - Wildcard SSL certificates are not issued under this root.
- Delegation of Domain / Email validation to third parties
    - Currently RA operation is not delegated to a third party. In the future JCSI may delegate RA operation to third party, but only after establishing the suitable control and audit procedure rules for external RAs.
- Issuing end entity certificates directly from roots
    - No. End-entity certs are issued through a subordinate CA.
- Allowing external entities to operate unconstrained subordinate CAs
    - There are no sub-CAs operated by third parties, and none planned.
- Distributing generated private keys in PKCS#12 files
    - No. According to the CPS the subscriber generates the private keys for web server certificates.
- Certificates referencing hostnames or private IP addresses
    - Web server certificates are not issued to hostnames or IP addresses.
- OCSP Responses signed by a certificate under a different root
    - No OCSP
- CRL with critical CIDP Extension
    - The CRLs download without error into Firefox.
- Generic names for CAs
    - "SecureSign" is the product trademark owned by JCSI, registered in Japan.

Verify Audits

(Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)

- Validate contact info in report, call to verify that they did indeed issue this report.
    - Posted on cert.webtrust.org
- For EV CA's, verify current WebTrust EV Audit done.
    - Not EV
- Review Audit to flag any issues noted in the report
    - No issues noted in report.