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 (English version)	http://www.jcsinc.co.jp/english/index.html
Organizational type	Public Commercial CA
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?)	Please provide a description of the JCSI company.

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

Info Needed	Data
Certificate Name	SecureSign RootCA11
Cert summary / comments	issues SSL enabled web server certificates to public end entities from subordinate issuing CA,
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)	For testing purposes, please provide a URL to a website whose certificate chains up to this root. Note that this can be a test site.
CRL URL	http://ssignadcrl01.jcsinc.co.jp/repository/crl/rca.crl http://ssignadcrl02.jcsinc.co.jp/repository/crl/rca.crl Need URL for CRL for end-entity certs. Need nextUpdate for end-entity certificates

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, which can be downloaded from: https://www2.jcsinc.co.jp/repository/certs/SSAD-sca1.der Are there any other internally operated subordinate CAs for this roots?
Subordinate CAs operated by third parties	Does this root have any subordinate CAs that are or will be operated by external third parties?
List any other root CAs that have issued cross-signing certificates for this root CA	Has this root been involved in cross-signing with any other root CAs?
Requested Trust Bits One or more of: • 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	Do you perform identity/organization verification for all SSL certificates? Or is it ever the case for SSL certs that the domain name is verified, but the identity/organization of the subscriber is not verified? • DV – only the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. • OV – in addition to verifying ownership/congrol of the domain name, the value of the Organization attribute is verified to be that associated with the certificate subscriber.
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 Public Service Standard in English: https://www2.jcsinc.co.jp/repository/SecureSignCPSv1.58-en.pdf Is this document relevant? Please review the potentially problematic practices, as per http://wiki.mozilla.org/CA:Problematic_Practices. Provide further information when relevant.
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
    - According to CPS:
        - Subscriber Web server certificates are valid for 1 year
        - Subscriber Long-term certificates may be valid for 11 years (What is this?)
        - Subscriber (other than the above) may be valid for 6 years (What is this?)
- Wildcard DV SSL certificates
    - Not found
- Delegation of Domain / Email validation to third parties
    - 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
    - ?

- Distributing generated private keys in PKCS#12 files
  - No. According to the CPS the subscriber generates the private keys.
- Certificates referencing hostnames or private IP addresses
  - Not found
- OCSP Responses signed by a certificate under a different root
  - No OCSP
- CRL with critical CIDP Extension
  - ?
- Generic names for CAs

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.