Bugzilla ID: 420705 (replaces original request of #382158, which expired)
Bugzilla Summary: add Comsign CA certs

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	ComSign LTD
Website URL (English version)	http://www.comsign.co.il/eng/default.asp
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	Private Corporation
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?)	ComSign is a private company owned by Comda, Ltd., a company specializing in information protection products and solutions. In 2003, ComSign was appointed by the Justice Ministry as a certificate authority in Israel in accordance with the Electronic Signature Law 5761-2001, and is currently the only entity issuing legal authorized electronic signatures according to the Israel law. ComSign has issued electronic signatures to thousands of business people in Israel.

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

Info Needed	Data	Data	Status / Notes
Certificate Name	ComSign CA	ComSign Secured CA	COMPLETE
Cert summary / comments	This root has six internally-operated subordinate CAs that are used for issuing digital ID's to individuals and corporations in accordance with the Israeli Electronic Signature Law.	This root has two internally-operated subordinate CAs that are used for issuing certificates for SSL and for code-signing.	COMPLETE
The root CA certificate URL Download into FireFox and verify	http://fedir.comsign.co.il/cert/comsignca.crt	http://fedir.comsign.co.il/cacert/ComsignSecuredCA.crt	COMPLETE
SHA-1 fingerprint.	E1:A4:5B:14:1A:21:DA:1A:79:F4:1A:42:A9:61:D6:69:CD:06:34:C1	F9:CD:0E:2C:DA:76:24:C1:8F:BD:F0:F0:AB:B6:45:B8:F7:FE:D5:7A	COMPLETE
Valid from	2004-03-24	2004-03-24	COMPLETE

Valid to	2029-03-19	2029-03-16	COMPLETE
Cert Version	3	3	COMPLETE
Modulus length / key length or type of signing key (if ECC)	2048	2048	COMPLETE
CRL • URL • update frequency for end-entity certificates	http://fedir.comsign.co.il/crl/ComSignCA.crl CRL issuing frequency for end-entity certificates: 24 Hours CPS Section 4.4.2: "ComSign will publish a new CRL the earliest of not later than every 24 hours or immediately following revocation of a certificate."	http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl CRL issuing frequency for end-entity certificates: 24 Hours	COMPLETE Comment #10: We removed the critical flag from the CRL. I still see the problem in Firefox. Perhaps this is because the CRLs were generated in October with the critical flag, and are next due to be generated in April? Comment #15: YES. by the law of the sate of Israel we need to cr8 new CRL every 6 month. We can not change the date. Next CRL will publish at April 2009.
OCSP (if applicable) • OCSP Responder URL • Max time until OCSP responders updated to reflect end-entity revocation	None	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.)	Cert Hierarchy Diagram: https://bugzilla.mozilla.org/attachment.cgi?id=346012 Comsign CA -> Bank leumi CA -> Corporate CA -> Corporations -> Clalit CA -> Leumi -> Comsign GOI	Comsign Secured CA -> Comsign Server CA -> Organization CA	COMPLETE

For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CPS, and that any audit covers them as well as the root.	"The subordinate are: Magna; Corporations; Bank Leumi; Clalit. The subordinate sign class 2 certificates. All certificates are by the Israeli law. we are the only public CA of Israel."		
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.	None	None Not allowed by the Israeli law	COMPLETE
List any other root CAs that have issued cross-signing certificates for this root CA	None	None	COMPLETE
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Email	Websites Code	COMPLETE
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • 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	IV, OV	OV	COMPLETE

the Organization attribute is verified to be that associated with the certificate subscriber. (This is commonly referred to as an OV certificate.)			
If EV certificates are issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.	N/A	N/A	Not Applicable
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.	https://bugzilla.mozilla.org/attachment.cgi?id=346499	https://www.4x4.co.il https://www.benezer.co.il/	COMPLETE
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	ComSign CPS Web Page www.comsign.co.il/cps Certification Practice Statement (CPS) http://www.comsign.co.il/CPS/English_CPS_final.pdf Security Certificate Approval Regulations For SSL Websites http://www.comsign.co.il/Images/Doc/CPS__SSL_EN.pdf		COMPLETE

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.)	Audit Type: Israel Electronic Signature Law Auditor: The State of Israel – Ministry of Justice Auditor website: http://www.justice.gov.il/MOJEng/Certification+Authorities+Registrar Registered CA: http://www.justice.gov.il/MOJEng/Certification+Authorities+Registrar/Registered+CAs/ Audit Type: ETSI TS 101 456 Auditor: Sharony-Shefler & CO Auditor Website: http://srsfcpa.co.il https://bugzilla.mozilla.org/attachment.cgi?id=348789 Letter Stating Compliance: https://bugzilla.mozilla.org/attachment.cgi?id=347141	COMPLETE Received email on 11/18 from the auditor, Mr. Shefler, verifying the authenticity of the audit letter. Received email on 12/16 from the Certification Coordinator at ISACA in regards to Mr. Shefler: "His ISACA ID number is 097621."

Review CPS sections dealing with subscriber verification (COMPLETE)

- Verify domain check for SSL
    - Section 3.1 of http://www.comsign.co.il/Images/Doc/CPS__SSL_EN.pdf, Requirements regarding verifying requests to issue a certificate
- 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.
    - CPS (http://www.comsign.co.il/CPS/English_CPS_final.pdf) Section 3.2: ComSign and\or its representatives will verify that –
        - 3.2.1.3. The information to be registered in the certificate is accurate, according to the details provided by the applicant;
    - CPS Section 4.1.2: *Required information:* 8) Email address.
- Verify identity info in code signing certs is that of subscriber
    - CPS Section 3 and 4.
- Make sure it's clear which checks are done for which context (cert usage)
    - Separate document for SSL

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

- 1.1 Long-lived DV certificates
    - CPS Section 4.2.3: One year
    - The SSL certs are OV
- 1.2 Wildcard DV SSL certificates
    - Not Found

    - The SSL certs are OV
- 1.3 Issuing end entity certificates directly from roots
    - No
- 1.4 Allowing external entities to operate unconstrained subordinate CAs
    - No subordinate CAs operated by third parties.
- 1.5 Distributing generated private keys in PKCS#12 files
    - CPS Section 4.1.4: "The key pair created by the applicant…"
- 1.6 Certificates referencing hostnames or private IP addresses
    - Not Found
- 1.7 OCSP Responses signed by a certificate under a different root
    - Not Applicable
- 1.8 CRL with critical CIDP Extension
    - The critical flag for CIDP Extension has been removed from the CRL, which will be re-generated in April, 2009.

Verify Audits (COMPLETE)
(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.
    - Verified
- For EV CA's, verify current WebTrust EV Audit done.
    - N/A
- Review Audit to flag any issues noted in the report
    - No issues noted