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
Certificate Name	ComSign CA	ComSign Secured CA
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.
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
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
Valid from	2004-03-24	2004-03-24

Valid to	2029-03-19	2029-03-16
Cert Version	3	3
Modulus length / key length or type of signing key (if ECC)	2048	2048
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
CRL download into Firefox	The current CRLs result in the ffffe009 error code when downloading into Firefox. ComSign has removed the critical flag from the CRL, and the new CRLs will be generated in April. 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)	None	None
List or description of subordinate CAs operated by the CA organization associated with the root CA For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CPS, and that any audit covers	Cert Hierarchy Diagram: https://bugzilla.mozilla.org/attachment.cgi?id=346012 Comsign CA -> Bank leumi CA -> Corporate CA -> Corporations -> Clalit CA -> Leumi -> Comsign GOI "The subordinate are: Magna; Corporations; Bank Leumi;	Comsign Secured CA -> Comsign Server CA -> Organization CA

them as well as the root.	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	None	None Not allowed by the Israeli law
List any other root CAs that have issued cross-signing certificates for this root CA	None	None
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Email	Websites Code
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. (DV) • Whether or not the value of the Organization	Not SSL IV, OV Comsign issues certificates according to Israeli law, which requires that they identify the person face to face, including checking his Israeli ID and driving license (or passport).	OV

attribute is verified to be that associated with the certificate subscriber. (OV)		
EV policy OID(s)	Not EV	Not EV
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable.	https://bugzilla.mozilla.org/attachment.cgi?id=346499	https://www.4x4.co.il https://www.benezer.co.il/
CP/CPS	ComSign CPS Web Page http://www.comsign.co.il/main.asp?id=125 Certification Practice Statement (CPS) http://www.comsign.co.il/Images/Doc/English_CPS_final.doc Security Certificate Approval Regulations For SSL Websites http://www.comsign.co.il/Images/Doc/CPS__SSL_EN.pdf	
AUDIT	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 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
    - From SSL CPS (http://www.comsign.co.il/Images/Doc/CPS__SSL_EN.pdf) section 3.1 Requirements regarding verifying requests to issue a certificate**:** Upon receipt of a request to issue a security certificate, the following inspections are performed: The certificate authority will confirm that:
        - (a) The organization requesting the certificate is registered and the company still in operation by one of the following:
            - a. Checking the organization's registration in the D&B website.
            - b. Checking the organization's registration at the registrar of companies/fellowship societies.
            - c. Receiving an official document from the certified authority confirming the organization's existence.
        - (b) An investigation will be performed to confirm that the domain for which the certificate is requested is registered in the organization's name.
        - (c) A telephone call will be made to the organization in order to verify the order and confirm the contact people's details as provided to ComSign.
- 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.
    - From CPS (http://www.comsign.co.il/Images/Doc/English_CPS_final.doc) section 3.2.1. Requirements related to Verifying Certificate Applications: When a request for a certificate issuing is received (according to chapter 4 of the procedures), ComSign will perform all required verification checks as a preliminary requirement for certificate issuing (according to chapter 3 and according to the Law and its regulations) as follows: ComSign and\or its representatives will verify that –
        - 3.2.1.1. The applicant signed the subscription agreement;
        - 3.2.1.2. The applicant is the person, corporation or public institute that has been identified in the application (in case of a corporation and\or public institute, see the detailed identification method in section 3.1 above);
        - 3.2.1.3**.** The information to be registered in the certificate is accurate, according to the details provided by the applicant;
        - 3.2.1.4**.** Authorized signers applying for a certificate on behalf of a corporation and\or public institute are legally permitted to submit such an application (see corporation or public institute identification method as specified in section 3.1 above). After the certificate has been issued, ComSign will not be responsible to continue and check and investigate the accuracy and correctness of the information included in the certificate issuing request, unless a notification will be sent to ComSign that the certificate was compromised.
        - 3.2.1.5 Comsign and /or its representatives will verify that the E-mail address is valid by sending mail to the costumer and ask him to reply.
- 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