Bugzilla ID: 675060
Bugzilla Summary: Add Comsign Global Root CA certificate

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	ComSign
Website URL	http://www.comsign.co.il/eng/default.asp
Organizational type	Private Corporateion
Primark Market / Customer Base	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.
CA Contact Information	CA Email Alias: support@comsign.co.il CA Phone Number: 972-3-6443620 Title / Department: SSL Product Manager

Technical information about each root certificate

Certificate Name	ComSign Global Root CA

Certificate Issuer Field	CN = ComSign Global Root CA
	O = ComSign Ltd.
	C = IL

Certificate Summary	This root will eventually replace the "ComSign CA" root certificate that is currently included in NSS, and was approved in bug #420705.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=549246
SHA1 Fingerprint	AE:3B:31:BF:8F:D8:91:07:9C:F1:DF:34:CB:CE:6E:70:D3:7F:B5:B0
Valid From	2011-07-18
Valid To	2036-07-16
Certificate Version	3
Certificate Signature Algorithm	PKCS #1 SHA-256 With RSA Encryption
Signing key parameters	4096
Test Website URL (SSL)	Test website or (if not requesting SSL trust bit) test certificate will be needed before this request reaches the top of the queue for public discussion.
CRL URL	URI: http://fedir.comsign.co.il/crl/comsignglobalrootca.crl URI: http://crl1.comsign.co.il/crl/comsignglobalrootca.crl When I try to import either of these CRLs into my Firefox browser, I get Error Code:ffffe009

	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."
OCSP URL	None
Requested Trust Bits	Specify one or more of the following trust bits to be enabled for this root: Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	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).
EV Policy OID(s)	N/A. Not requesting EV treatment for this root.

CA Hierarchy information for each root certificate

CA Hierarchy	CA Hierarchy Diagram for the previously included roots: https://bugzilla.mozilla.org/attachment.cgi?id=346012 Please correct… This root will eventually replace the "ComSign CA" root certificate that is currently included in NSS, as such, "ComSign Global Root CA" will eventually have the following internally-operated subordinate CAs: -> Bank leumi CA -> Corporate CA -> Corporations -> Clalit CA -> Leumi -> Comsign GOI
Externally Operated SubCAs	If this root has subCAs that are operated by external third parties, then provide the information listed here: https://wiki.mozilla.org/CA:SubordinateCA_checklist If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.
Cross-Signing	List all other roots for which this root CA has issued cross-signing certificates. List all other root CAs that have issued cross-signing certificates for this root CA. Note whether the roots in question are already included in the Mozilla root store or not.

Verification Policies and Practices

Policy Documentation	ComSign CPS Web Page: http://www.comsign.co.il/main.asp?id=125 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
Audits	Audit Type: ETSI TS 101 456 Auditor: Sharony-Shefler Auditor Website: https://bugzilla.mozilla.org/attachment.cgi?id=348789 URL to Audit Report: https://bug420705.bugzilla.mozilla.org/attachment.cgi?id=541112 (2011.02.10) Note: Final approval will be dependent on there being an updated audit that includes this new root.

	Audit Type: Israel Electronic Signature Law The State of Israel – Ministry of Justice: http://www.justice.gov.il/MOJEng/Certification+Authorities+Registrar Registered CA: http://www.justice.gov.il/MOJEng/Certification+Authorities+Registrar/Registered+CAs/
Organization Verification Procedures	Excerpt from CPS: http://www.comsign.co.il/Images/Doc/English_CPS_final.doc 3. Identification and Authentication 3.1. Initial Registration 3.1.1. Identifying a Single Applicant for a First Certificate Issue: 3.1.1.1. A single applicant which is an Israeli resident – using an identity card and a valid Israeli passport or a valid Israeli driving license containing a photo and information received from the population department of the ministry of the interior ("population registry") containing the following details: identity number of applicant, last name and previous last name if exists, father name, mother name, year of birth, date last identity card was issued, reason for this issue, present address, and if relevant death status and date of death. 3.1.1.2. A single applicant living abroad – Using a foreign passport, a journey certificate or an identity card, and an additional identification document containing the applicant's photo and identifying details of him\her and the entity that issued the additional document. 3.1.2. Identifying Corporations and\or Public Institutes for a First Certificate Issue: 3.1.2.1. A corporation registered in Israel – According to the incorporation certificate, a lawyer statement confirming the existence of the corporation, its name and registered number, or instead of a lawyer approval as specified – by verifying in the proper registries and according to certified copy of the corporation resolution on authorized signatories of the corporation, or a lawyer's statement stating the identity of such authorized signer. 3.1.2.2. A corporation not registered in Israel – By an approved copy of a document stating that the corporation has been incorporated, a lawyer statement confirming the existence of the corporation, its name and registered number, or instead of a lawyer approval as specified – by verifying in the proper registries and according to certified copy of the corporation resolution on authorized signatories of the corporation, or a lawyer's statement stating the identity of such authorized signer. 3.1.2.3. A public institution – According to the applicant statement, after the CA has been notified by a document, that the authorized signer may act on behalf of the public institution. For this matter, a "public institution" – governmental offices, local authorities and authorities, corporations or additional institutions established in Israel by law. 3.1.2.4. As for corporations (registered or not registered in Israel) and public institutes – the CA will identify the authorized signer using the same methods used to identify a single Israeli citizen or a foreign resident, as required and detailed in section 3.1.1 above. 3.1.2.5. For a corporation which is not registered in Israel or a public institution – an "authorized copy" is required – a copy identical to the original verified by one of the following entities: 3.1.2.5.1. The authority issuing the original document. 3.1.2.5.2. A licensed Lawyer approved for jurisprudence in Israel. 3.1.2.5.3. An Israeli diplomatic or consular representative abroad.

	3.2. Validating Requests for Certificate Issue 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 replay. 3.2.2. Personal presence To ensure the identification of the applicant and to verify the relation between the applicant and his\her public key, Regulation 10 to the Electronic Signature Regulations (hardware and software systems) states that single and\or authorized signers of corporations applying for an electronic certificate must appear in person in front of ComSign and\or any of its representatives.
SSL Verification Procedures	Excerpt from Security Certificate Approval Regulations For SSL Websites: http://www.comsign.co.il/Images/Doc/CPS_SSL_EN.pdf 3. Verification of certificate issuing requests 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 a 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.
Email Address Verification Procedures	CPS section 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 replay.
Code Signing Subscriber Verification Procedures	I did not see any mention of Code Signing certificates in the CPS documents. If you are requesting that the code signing trust bit be enabled, then there must be supporting documentation for the verification and issuance of code signing certificates.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	CPS documents are publicly available.
CA Hierarchy	Need information about what the hierarchy will be.
Audit Criteria	ETSI TS 101 456
Document Handling of IDNs in CP/CPS	Are international domain names (IDNs) allowed in SSL certs chaining up to this root?
Revocation of Compromised Certificates	CPS section 4.4
Verifying Domain Name Ownership	See details above.
Verifying Email Address Control	See details above.
Verifying Identity of Code Signing Certificate Subscriber	I didn't see reference to code signing certs in the CPS.
DNS names go in SAN	?
Domain owned by a Natural Person	?
OCSP	Not provided

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	SSL certs are OV CP section 4.2.3: end-entity cert validity period is one year.
Wildcard DV SSL certificates	Not found.
Email Address Prefixes for DV Certs	SSL certs are OV
Delegation of Domain / Email validation to third parties	Is email or domain validation ever delegated to external third parties?
Issuing end entity certificates directly from roots	
Allowing external entities to operate subordinate CAs	Will there ever by externally operated subCAs chaining up to this root?
Distributing generated private keys in PKCS#12 files	CPS section 4.1.4: The key pair created by the applicant must conform to regulation 8 of the electronic signatures regulations (hardware and software systems) as follows: "The electronic signature is produced using a key based on a common standard which uses one of the following: (1) RSA or DSA key which is at least 1024 bits, (2) Elliptic curve DSA key which is at least 160 bits".
Certificates referencing hostnames or private IP addresses	Not found
Issuing SSL Certificates for Internal Domains	?
OCSP Responses signed by a certificate under a different root	OCSP not provided
CRL with critical CIDP Extension	?
Generic names for CAs	CN and O include ComSign