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
Cert Signature Algorithm	PKCS #1 SHA-256 With RSA Encryption
Signing key parameters	4096
Test Certificate	Intermediate Cert: https://bugzilla.mozilla.org/attachment.cgi?id=613736 Test Cert: https://bugzilla.mozilla.org/attachment.cgi?id=613738
CRL URL	URI: http://fedir.comsign.co.il/crl/comsignglobalrootca.crl URI: http://crl1.comsign.co.il/crl/comsignglobalrootca.crl CPS Section 2.3: ComSign will publish a new list of revoked certificates no later than every 12 hours or immediately after a certificate is revoked, whichever is earlier. The published list of revoked certificates is valid for 24 hours.

OCSP URL	None
Requested Trust Bits	Email (S/MIME)
SSL Validation Type	IV. 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: https://bugzilla.mozilla.org/attachment.cgi?id=551315 "ComSign Global Root CA" will eventually have the following internally-operated subordinate CAs: - ComSign ISA Global CA - ComSign Corporations CA - ComSign Professionals CA
Externally Operated SubCAs	None, and none planned.
Cross-Signing	None, and none planned.

Verification Policies and Practices

Policy Documentation	Document Repository: http://www.comsign.co.il/main.asp?id=114 CPS (English): http://www.comsign.co.il/CPS-Docs/CPS_Ver3-1_English.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://bugzilla.mozilla.org/attachment.cgi?id=8505604 (2014.09.16) 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/
Identity Verification Procedures	CPS sections 3.2 and 3.3
SSL Verification Procedures	N/A – Not requesting the websites trust bit.
Email Address Verification Procedures	CPS section 3.2.7.1: As part of the identification process, a unique secret code (the "Secret Code" will be mailed by Comsign to the Applicant's e-mail address. The Secret Code will be mailed during the coordination stage preceding the Applicant's personal appearance for the identification process. The Applicant will provide the Secret Code to the coordination clerk during the telephone conversation coordinating the Applicant's personal appearance. If the provided Secret Code is correct, the coordination clerk will transfer it to the identification clerk together with all other data pertaining to the applicant (including the applicant's e-mail address). CPS section 3.2.7.2: In the event of a non-coordinated visit to Comsign offices (as well as in any other event) the identification clerk will mail the Secret Code during the identification process (Comsign will provide the Applicant with internet access).

	CPS section 3.2.7.3: The Applicant must provide the Secret Code in the application form. The identification clerk will verify the matching of the Secret Code in the application form with the one reported by the coordination clerk (or by the applicant himself in a non-coordinated visit to Comsign offices) as well as the matching of the e-mail address in the application form with the address reported by the coordination clerk. Alternatively, the identification clerk will verify the matching of the Secret Code in the application form to the one mailed by the identification clerk to the e-mail address provided by the Applicant in the application form. CPS section 3.2.7.4: Only the e-mail address to which the verified Secret Code was mailed will appear in the electronic certificate issued by Comsign to the Applicant.
Code Signing Subscriber Verification Procedures	N/A – Not requesting the websites trust bit.

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	Root only signs internally-operated intermediate CAs.
Audit Criteria	ETSI TS 101 456
Document Handling of IDNs in CP/CPS	
Revocation of Compromised Certificates	CPS section 4.8
Verifying Domain Name Ownership	N/A
Verifying Email Address Control	See details above.
Verifying Identity of Code Signing Certificate Subscriber	N/A
DNS names go in SAN	N/A
Domain owned by a Natural Person	N/A
OCSP	Not provided

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

Long-lived DV certificates	N/A – Not requesting websites trust bit.
Wildcard DV SSL certificates	N/A
Email Address Prefixes for DV Certs	N/A
Delegation of Domain / Email validation to third parties	No
Issuing end entity certificates directly from roots	No
Allowing external entities to operate subordinate CAs	No
Distributing generated private keys in PKCS#12 files	CPS section 4.5.2: 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	Not found

private IP addresses	
Issuing SSL Certificates for Internal Domains	N/A
OCSP Responses signed by a certificate under a different root	OCSP not provided
CRL with critical CIDP Extension	CRLs import into FF browser without error.
Generic names for CAs	CN and O include ComSign