

Mozilla - CA Program

Case Information			
Case Number	00000008	Case Record Type	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	ComSign	Request Status	Need Information from CA

Additional Case Information			
Subject	Include renewed root	Case Reason	New Owner/Root inclusion requested

Bugzilla Information	
Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=675060

General information about CA's associated organization			
CA Email Alias 1	support@comsign.co.il		
CA Email Alias 2			
Company Website	http://www.comsign.co.il/eng/default.asp	Verified?	Verified
Organizational Type	Private Corporation	Verified?	Verified
Organizational Type (Others)		Verified?	Not Applicable
Geographic Focus	Israel	Verified?	Verified
Primary Market / Customer Base	ComSign is owned by Comda, Ltd., and was appointed by the Justice Ministry as a CA in Israel in accordance with the Electronic Signature Law 5761-2001. ComSign has issued electronic signatures to thousands of business people in Israel.	Verified?	Verified
Impact to Mozilla Users	This request is to include the SHA-256 ComSign CA root certificate that is currently included in NSS.	Verified?	Verified

Response to Mozilla's list of Recommended Practices			
Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	Recommended Practices Statement	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	* CA Hierarchy -- Root only signs internally-operated intermediate CAs. * Revocation of Compromised Certificates -- CPS section 4.8	Verified?	Verified

Response to Mozilla's list of Potentially Problematic Practices			

Potentially Problematic Practices https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices

Problematic Practices Statement I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.

CA's Response to Problematic Practices	<ul style="list-style-type: none"> * SSL certificates maximum validity period – 3 years * Wildcard DV SSL certificates – are issued based on the specifications in CA/B forum BR section 11.1.3. * 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". 	Verified?	Verified
---	--	------------------	----------

Root Case Record # 1

Root Case Information

Root Certificate Name	ComSign Global Root CA	Root Case No	R00000013
Request Status	Need Information from CA	Case Number	00000008

Additional Root Case Information

Subject	Include ComSign Global Root CA
----------------	--------------------------------

Technical Information about Root Certificate

O From Issuer Field	ComSign Ltd.	Verified?	Verified
OU From Issuer Field		Verified?	Verified
Certificate Summary	This root will eventually replace the "ComSign CA" root certificate that is currently included in NSS, and was approved in bug #420705.	Verified?	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=549246	Verified?	Verified
Valid From	2011 Jul 18	Verified?	Verified
Valid To	2036 Jul 16	Verified?	Verified
Certificate Version	3	Verified?	Verified
Certificate Signature Algorithm	SHA-256	Verified?	Verified
Signing Key Parameters	4096	Verified?	Verified
Test Website URL (SSL) or Example Cert	https://fedir.comsign.co.il/test.html	Verified?	Verified
CRL URL(s)	http://fedir.comsign.co.il/crl/ComSignGlobalRootCA.crl http://fedir.comsign.co.il/crl/ComsignOrganizationalCa.crl CPS Section 2.3: The published list of revoked certificates is valid for 24 hours.	Verified?	Verified
OCSP URL(s)	http://ocsp1.comsign.co.il	Verified?	Verified

Revocation Tested	http://certificate.revocationcheck.com/fedir.comsign.co.il NEED: Fix reported errors (items marked with "x" and in red).	Verified?	Need Response From CA
Trust Bits	Code; Email; Websites	Verified?	Verified
SSL Validation Type	DV; OV	Verified?	Verified
EV Policy OID(s)	Not EV	Verified?	Not Applicable
EV Tested	Not requesting EV treatment at this time.	Verified?	Not Applicable
Root Stores Included In	Microsoft	Verified?	Verified
Mozilla Applied Constraints	None	Verified?	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	AE:3B:31:BF:8F:D8:91:07:9C:F1:DF:34:CB:CE:6E:70:D3:7F:B5:B0	Verified?	Verified
SHA-256 Fingerprint	26:05:87:5A:FC:C1:76:B2:D6:6D:D6:6A:99:5D:7F:8D:5E:BB:86:CE:12:0D:0E:7E:9E:7C:6E:F2:94:A2:7D:4C	Verified?	Verified

CA Hierarchy Information

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	Verified?	Verified
Externally Operated SubCAs	None, and none planned.	Verified?	Verified
Cross Signing	None, and none planned.	Verified?	Verified
Technical Constraint on 3rd party Issuer	CPS section 3.2.8, Authentication Process for SSL certificates: "All authentication and verification procedures in this sub-section will be performed either directly by ComSign's personnel (RAOs) or by ComSign's authorized representatives. NEED: Can someone external to ComSign directly cause the issuance of an SSL certificate? If yes, what procedure/controls are in place for external RAs in regards to SSL certificate issuance?	Verified?	Need Clarification From CA

Verification Policies and Practices

Policy Documentation	Document Repository (Hebrew): http://www.comsign.co.il/main.asp?id=114 Document Repository (English): https://www.comsign.co.uk/?page_id=1282	Verified?	Verified
CA Document Repository	https://www.comsign.co.uk/	Verified?	Verified

CP Doc Language	English		
CP	https://www.comsign.co.uk/?page_id=1282	Verified?	Verified
CP Doc Language	English		
CPS	http://www.comsign.co.uk/wp-content/uploads/Comsign%20CPS-EN-v%20311.pdf	Verified?	Verified
Other Relevant Documents	<p>Ministry of Justice Registered CA: http://www.justice.gov.il/MOJEng/Certification+Authorities+Registrar/Registered+CAs/</p> <p>Only the Hebrew version of the CPS was approved by the Israeli CA Registrar. The English version of the CPS adds procedures dealing with SSL certificates, which are not regulated under Israel's Electronic Signature Law.</p>	Verified?	Verified
Auditor Name	Sharony-Shefler	Verified?	Verified
Auditor Website	http://srscpa.co.il/	Verified?	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx	Verified?	Verified
Standard Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8599627	Verified?	Verified
Standard Audit Type	WebTrust	Verified?	Verified
Standard Audit Statement Date	4/26/2015	Verified?	Verified
BR Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8598250	Verified?	Verified
BR Audit Type	WebTrust	Verified?	Verified
BR Audit Statement Date	4/26/2015	Verified?	Verified
EV Audit	Not requesting EV treatment	Verified?	Not Applicable
EV Audit Type		Verified?	Not Applicable
EV Audit Statement Date		Verified?	Not Applicable
BR Commitment to Comply	English CPS section 1	Verified?	Verified
SSL Verification Procedures	<p>Note: The English version of the CPS adds procedures dealing with SSL certificates, which are not regulated under Israel's Electronic Signature Law. So, the SSL verification procedures are only part of the English version of the CPS.</p> <p>CPS section 3.2.8.1: For issuing certificates to organizations requesting SSL certificates, Comsign performs domain name owner verification to detect cases of homographic spoofing of IDNs. Comsign employs an automated or manual process that searches various 'whois' services to find the owner of a particular domain. A search failure result is flagged and the RA rejects the Certificate Request. Additionally, the RA rejects any domain name that visually appears to be made up of multiple scripts within one hostname label.</p> <p>Note: Orders for major corporations, well</p>	Verified?	Verified

known trademarks and financial institutions may be queued for further security reviews prior to issuance. In the event an order is queued for review the administrative contact must be a full time employee of the company for successful issuance. A verification telephone call with the administrative contact may be required.
 - Verification methods include one of the following:
 3.2.8.1.1 EMail-based DCV
 3.2.8.1.2 DNS-based DCV
 3.2.8.1.3 HTTP(S)-based DCV

EV SSL Verification Procedures	Not requesting EV treatment at this time. CPS section 3.2.8.2 - 3.2.8.3 – EV	Verified?	Not Applicable
Organization Verification Procedures	CPS sections 3.2.1 - Identifying an individual 3.2.2 - Identifying an Authorized Signatory of a Corporation and/or Public Institution 3.2.8.2 - Authentication of Organization identity (SSL)	Verified?	Verified
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). See details in CPS sections 3.2.7.2 and 3.2.7.3. 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.	Verified?	Verified
Code Signing Subscriber Verification Pro	CPS section 3.2.9: Authentication Process for Code Signing Certificates	Verified?	Verified
Multi-Factor Authentication	CPS section 5	Verified?	Verified
Network Security	CPS sections 5 and 6	Verified?	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://www.comsign.co.uk/?page_id=1306	Verified?	Verified
--	---	-----------	----------