Bugzilla ID: 851435
Bugzilla Summary: WoSign two root certificate inclusion application

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	WoSign eCommerce Services Limited, DBA: WoSign
Website URL	www.wosign.com
Organizational type	Private corporation
Primark Market / Customer Base	Types of customers: General public Vertical market segments: No. Applicable to all market segments. Geographic region? Starting in China market, with plans to expand into Japan and Korea.
Impact to Mozilla Users	WoSign is a private-owned CA in China which issues certificates to the general public. WoSign started their CA business in 2006 as a SubCA of Comodo. WoSign setup its own root CA in 2009 and started to issue certificates in 2011 under this root CA that cross signed with a Startcom CA. WoSign has issued thousands of certificates to China customers, WoSign SSL certificates are deployed in top 10 eCommerce websites in China; for bank, telecom, enterprise etc., and most software developers in China choose WoSign certificate since it supports Chinese. Currently, there are 3 state–owned CAs in China that joined this Program. We think the market needs a commercial CA to provide best products and best service; WoSign is a private owned company that has engaged in CA business for 8 years. We have the PKI technology mastered R&D team, identity authentication team with rich experience and excellent technical support and customer service team. We are sure we will be one of the leaders in China, and we are planning to expand to Japan and Korea market that also have the strong request to issue local language certificates that we support like Japanese and Korean.
Inclusion in other major browsers	Applying with Mozilla, Microsoft, Apple at the same time.
CA Contact Information	CA Email Alias: ca@wosign.com CA Phone Number: +86-755-26027858, 86008688 Title / Department: Mr. Richard Wang, CTO

Technical information about each root certificate

Certificate Name	Certification Authority of WoSign	CA WoSign
Certificate Issuer Field	CN = Certification Authority of WoSign O = WoSign eCommerce Services Limited C = CN	CN = CA WoSign O = WoSign eCommerce Services Limited C = US

Certificate Summary	This root has internally-operated intermediate certificates that issue SSL, Code Signing, and Client certificates for individuals and organizations.	This root has internally-operated intermediate certificates that issue SSL, Code Signing, and Client certificates for individuals and organizations.
Root Cert URL	http://www.wosign.com/Root/ca1.crt	http://www.wosign.com/Root/ws_ca2.crt
SHA1 Fingerprint	33:A4:D8:BC:38:60:8E:F5:2E:F0:E2:8A:35:09:1E:92:50:90:7F:B9	AF:F5:F5:BD:B7:CF:2B:6D:0C:FB:2D:6A:2A:95:9A:07:CE:34:33:8B
Valid From	2009-08-08	2009-08-08
Valid To	2039-08-08	2039-08-08
Certificate Version	3	3
Cert Signature Algorithm	PKCS #1 SHA-1 With RSA Encryption	PKCS #1 SHA-256 With RSA Encryption
Signing key parameters	4096	4096
Test Website URL (SSL)	https://root1evtest.wosign.com	Will provide latter since we don't issue any cerificate from this root CA now
CRL URL	http://crls.wosign.com/ca.crl http://crls.wosign.com/server-4.crl (NextUpdate: 24 hours) http://crls.wosign.com/server-3.crl (NextUpdate: 24 hours) http://crls.wosign.com/server-1.crl (NextUpdate: 24 hours) http://crls.wosign.com/client-1.crl http://crls.wosign.com/client-2.crl http://crls.wosign.com/client-3.crl http://crls.wosign.com/code-3.crl WoSign updates and publishes a new CRL every 24 hours or whenever a CA Certificate is revoked. The CRL of root and intermediate CA certificates may be valid for one year and shall be updated accordingly.	http://crls2.wosign.com/ca.crl http://crls2.wosign.com/server-4.crl http://crls2.wosign.com/server-3.crl http://crls2.wosign.com/server-1.crl http://crls2.wosign.com/client-1.crl http://crls2.wosign.com/client-2.crl http://crls2.wosign.com/client-3.crl http://crls2.wosign.com/code-3.crl WoSign don't setup those CRL server now.
OCSP URL (Required now)	http://ocsp.wosign.com/ca http://ocsp.wosign.com/class4/server/ca http://ocsp.wosign.com/class3/server/ca http://ocsp.wosign.com/class1/server/ca http://ocsp.wosign.com/class1/client/ca http://ocsp.wosign.com/class2/client/ca http://ocsp.wosign.com/class3/client/ca http://ocsp.wosign.com/class3/code/ca	http://ocsp2.wosign.com/ca http://ocsp2.wosign.com/class4/server/ca http://ocsp2.wosign.com/class3/server/ca http://ocsp2.wosign.com/class1/server/ca http://ocsp2.wosign.com/class1/client/ca http://ocsp2.wosign.com/class2/client/ca http://ocsp2.wosign.com/class3/client/ca http://ocsp2.wosign.com/class3/code/ca
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	DV, OV, and EV	DV, OV, and EV

EV Policy OID(s)	1.3.6.1.4.1.36305.2 Please complete the EV testing described here: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version And attach a screen shot to the bug that shows the EV treatment (green bar). See attached screenshot	1.3.6.1.4.1.36305.2 Please complete the EV testing described here: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version And attach a screen shot to the bug that shows the EV treatment (green bar).
Non-sequential serial numbers and entropy in cert	http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html "9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: ... all new endt entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number)." Yes, end-entity certificates serial number is random data with 7 bytes, and the issue time is random time, not the exact time.	http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html "9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: ... - all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number)."

CA Hierarchy information for each root certificate

CA Hierarchy	There are 7 internally-operated subordinate CAs for this root CA: (1) WoSign Class 4 EV Server CA (2) WoSign Class 3 OV Server CA (3) WoSign Class 1 DV Server CA (4) WoSign Class 3 Code Signing CA (5) WoSign Class 1 Client CA (6) WoSign Class 2 Client CA (7) WoSign Class 3 Client CA	??? Please provide CA Hierarchy information for "CA WoSign" root. N/A yet
Externally Operated SubCAs	None, and none planned.	??? None
Cross-Signing	Startcom CA (CN = StartCom Certification Authority) issued crosst signing certificate for this root CA.	??? N/A
Technical Constraints on Third-party Issuers	External third parties may not cause the issuance of certificates in this CA hierarchy.	??? N/A

New CPS V1.2.1: http://www.wosign.com/policy/wosign-policy-1_2_1.pdf

Verification Policies and Practices

Policy Documentation	CPS (English): http://www.wosign.com/policy/WoSign-Policy-1_1.pdf
Audits	Audit Type: WebTrust for CA and WebTrust for EV Auditor: Ernst & Young Audit Report: https://cert.webtrust.org/ViewSeal?id=1443 (2013.01.15) EV Readiness Audit Report: https://bugzilla.mozilla.org/attachment.cgi?id=725294 (2013.01.15)
Baseline Requirements (SSL)	CPS section 1.3.1.2. Commitment to comply with applicable standards, will update to v1.2 "Comply BR" clearly. YES, in CPS V1.2.1

Organization Verification Procedures	CPS section 1.6.2: Class 1:Email address or domain name ownership/control verified. No identity checking. Class 2: Some identity checking. Class 3: Organization verified, phone call, trusted database checked. Class 4: EV CPS section 3.2.2.3.1 (Class 3): Organization verification CPS section 3.2.4: Validation of authority: WoSign confirms and verifies that the subscriber is duly authorized to represent the organization and obtain the certificate on their behalf by obtaining an authorization statement and by contacting the authorizer.
SSL Verification Procedures	CPS section 3.2.2.1.2 (Class 1, DV): Fully qualified domain names, typically www.domain.com or "domain.com" are validated by sending an electronic mail message with a verification code to one of the following administrative electronic mail accounts: webmaster@domain.com, hostmaster@domain.com, postmaster@domain.com The subscriber has to return and submit the verification code as prove of ownership of the domain name within a limited period sufficient enough to receive an electronic mail message. Additionally the existence of the domain name is verified by checking the WHOIS records provided by the domain name registrar. If the WHOIS data contain additional email addresses, they may be offered as additional choices to the above mentioned electronic mail accounts. CPS section 3.2.2.3.1 (Class 3, OV): Domain and email control validation is performed as in Class 1. Domain control may be also established through verification of the WHOIS records and matching subscriber information. CPS section 3.2.2.4 (Class 4, EV): Extended Validation for organizations are preformed according to the validation procedures and requirements of the Extended Validation Guidelines as published by the CA/Browser Forum. Applicants for EV must be at least Class 2 Identity validated **prior** to engagement for Extended validation.
Email Address Verification Procedures	CPS section 3.2.2.1.1 (Class 1): Email accounts are validated by sending an electronic mail message with a verification code to the requested email account. The subscriber has to return and submit the verification code as prove of ownership of the email account within a limited period sufficient enough to receive an electronic mail message. CPS section 3.2.2.2.1 (Class 2): Email control validation is performed as in Class 1.
Code Signing Subscriber Verification Procedures	Where in the CPS does it say that Object Code Signing Certificates are Class3? CPS V1.2.1 Page P17, 3.1.1.3; CPS V1.1: Page 9, 3.1.1.3
Multi-factor Authentication	CPS section 5.3. Client Certificate in USB Key.
Network Security	CPS sections 5 and 6.

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

Publicly Available CP and CPS	Yes. See above.
CA Hierarchy	Yes. See above.
Audit Criteria	Yes. See above.
Document Handling of IDNs in CP/CPS	??? CPS V1.2.1, Page 24, 3.2.2.1.2
Revocation of Compromised Certificates	CPS section 4.9
Verifying Domain Name Ownership	See above.
Verifying Email Address Control	See above.
Verifying Identity of Code Signing Certificate Subscriber	See above.
DNS names go in SAN	Yes
Domain owned by a Natural Person	DV certs are issued without identity/organization checking.
OCSP	Yes

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

Long-lived DV certificates	DV SSL certs are valid up to 2 years.
Wildcard DV SSL certificates	CPS section 3.2.2.1.2 (Class 1, DV): Wildcard domain names like "*.domain.com" are not issued in the Class 1 level.
Email Address Prefixes for DV Certs	If DV SSL certs, then list the acceptable email addresses that are used for verification: 4 Emails: webmaster@, hostmaster@, postmaster@ and Whois Admin email.
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	No
Certificates referencing hostnames or private IP addresses	No CPS section 3.2.2.1.3: Ipv4 addresses must bind to a FQDN and must not be reserved by IANA… The subscriber must provide attestation about the right to use the relevant IP addresses.
Issuing SSL Certificates for Internal Domains	No
OCSP Responses signed by a certificate under a different root	No
CRL with critical CIDP Extension	No
Generic names for CAs	No
Lack of Communication With End Users	No