Mozilla - CA Program

Case Information

Case Number	00000061	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	WoSign CA Limited	**Request Status**	Ready for Public Discussion

Additional Case Information

Subject	Include WoSign G2 and ECC Roots	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1156175

General information about CA's associated organization

CA Email Alias 1	ca@wosign.com		
CA Email Alias 2			
Company Website	http://www.wosign.com/	**Verified?**	Verified
Organizational Type	Commercial Organization	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	China	**Verified?**	Verified
Primary Market / Customer Base	WoSign SSL certificates are deployed in top 10 eCommerce websites in China; for bank, telecom, enterprise etc.	**Verified?**	Verified
Impact to Mozilla Users	WoSign's previous root certificates were included via Bug #851435. This request is to included the G2 and ECC roots.	**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	* Document Handling of IDNs in CP/CPS - CPS section 3.2.2.1.2 * Revocation of Compromised Certificates - CPS section 4.9	**Verified?**	Verified

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic	https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices**	I have reviewed Mozilla's list of Potentially Problematic

Practices		**Statement**	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	* DV SSL certs are valid up to 3 years. * CPS section 3.2.2.1.2: Wildcard domain names like "*.domain.com" are not issued in the Class 1 level. * If DV SSL certs, then list the acceptable email addresses that are used for verification: webmaster@, hostmaster@, postmaster@, admin@domain.com, administrator@domain.com and Whois Admin email. * 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.	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	Certification Authority of WoSign G2	**Root Case No**	R00000079
Request Status	Ready for Public Discussion	**Case Number**	00000061

Additional Root Case Information

Subject	Include Certification Authority of WoSign G2

Technical Information about Root Certificate

O From Issuer Field	WoSign CA Limited	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	This SHA-256 root cert will eventually replace the SHA-1 "Certification Authority of WoSign" root cert that was included via Bugzilla Bug #851435. It will have internally-operated intermediate certificates that issue certs to individuals and organizations	**Verified?**	Verified
Root Certificate Download URL	http://www.wosign.com/root/WS_CA1_G2.crt	**Verified?**	Verified
Valid From	2014 Nov 08	**Verified?**	Verified
Valid To	2044 Nov 08	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://root4evtest.wosign.com/	**Verified?**	Verified
CRL URL(s)	http://crls6.wosign.com/ca6.crl http://crls6.wosign.com/ca6-ssl4.crl CPS 7.8: CRL Next Update: 5 days	**Verified?**	Verified

OCSP URL(s)	http://ocsp6.wosign.com/ca6 http://ocsp6.wosign.com/ca6/ssl4	**Verified?**	Verified
Revocation Tested		**Verified?**	
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	1.3.6.1.4.1.36305.2	**Verified?**	Verified
EV Tested	// CN=Certification Authority of WoSign G2,O=WoSign CA Limited,C=CN "1.3.6.1.4.1.36305.2", "WoSign EV OID", SEC_OID_UNKNOWN, { 0xD4, 0x87, 0xA5, 0x6F, 0x83, 0xB0, 0x74, 0x82, 0xE8, 0x5E, 0x96, 0x33, 0x94, 0xC1, 0xEC, 0xC2, 0xC9, 0xE5, 0x1D, 0x09, 0x03, 0xEE, 0x94, 0x6B, 0x02, 0xC3, 0x01, 0x58, 0x1E, 0xD9, 0x9E, 0x16 }, "MFgxCzAJBgNVBAYTAkNOMRowGAYDVQQKExFXb1NpZ24gQ0EgTGltaXRlZDEtMCsG" "A1UEAxMkQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgb2YgV29TaWduIEcy", "ayXaioidfLwPBbOxemFFRA==", Success!	**Verified?**	Verified
Root Stores Included In		**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	FB:ED:DC:90:65:B7:27:20:37:BC:55:0C:9C:56:DE:BB:F2:78:94:E1	**Verified?**	Verified
SHA-256 Fingerprint	D4:87:A5:6F:83:B0:74:82:E8:5E:96:33:94:C1:EC:C2:C9:E5:1D:09:03:EE:94:6B:02:C3:01:58:1E:D9:9E:16	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	The plan is to have 10 internally-operated subCAs for 3 types of certificates: SSL Certificate, Code Signing Certificate and Client Certificate. 1. WoSign Class 4/3/2/1 EV/OV/IV/DV SSL CA G2 2. WoSign Class 4/3/2 EV/OV/IV Code Signing CA G2 3. WoSign Class 3/2/1 Client CA G2 Currently, one of the subCAs has been issued: WoSign Class 4 EV SSL CA G2	**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	External third parties may not cause the issuance of certificates in this CA hierarchy.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Document Repository (Chinese):	**Verified?**	Verified

	http://www.wosign.com/policy/cps.htm		
CA Document Repository	http://www.wosign.com/policy/cps_e.htm	**Verified?**	Verified
CP Doc Language			
CP		**Verified?**	Not Applicable
CP Doc Language			
CPS	http://www.wosign.com/policy/wosign-policy-1-2-12.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor Name	Ernst & Young (EY)	**Verified?**	Verified
Auditor Website	http://www.ey.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1843&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	2/28/2015	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1860&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	4/10/2015	**Verified?**	Verified
EV Audit	https://cert.webtrust.org/SealFile?seal=1842&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	2/28/2015	**Verified?**	Verified
BR Commitment to Comply	CPS section 1.2.	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2.1.2: Fully qualified domain names ... 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 - admin@domain.com - administrator@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 be the domain name registrar. If the WHOIS data contain an administrative email addresses, that may be offered as additional choice to the above mentioned electronic mail accounts. If the subscriber can't receive email from the above email account, he/she can choose to do the website control	**Verified?**	Verified

	validation that the subscriber must upload a website control validation code file to the website root directory to finish the website control validation. CPS section 3.2.2.3 (Class 3): Domain and email control validation is performed as in Class 1. Domain control may also be established through verification of the WHOIS records and matching subscriber information.		
EV SSL Verification Procedures	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.	**Verified?**	Verified
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.	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.2.1.1: 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 and electronic mail message. CPS section 3.2.2.2 (Class 2): Email control validation is performed as in Class 1.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	According to section 3.1.1 of the CPS, the validation levels allowed for Code Signing certs are Class 2, Class 3, or Class 4/EV. Steps taken to verify the identity of the certificate subscriber and verify the organization are described in section 3.2.2 of the CPS, and steps taken to verify the authority of the certificate subscriber to act on behalf of the organization are described in section 3.2.4.	**Verified?**	Verified
Multi-Factor Authentication	CPS section 5.3. Client Certificate in USB Key.	**Verified?**	Verified
Network Security	CPS sections 5 and 6	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://www.wosign.com/english/root.htm	**Verified?**	Verified

Root Case Record # 2

Root Case Information

Root Certificate Name	CA WoSign ECC Root	**Root Case No**	R00000080
Request Status	Ready for Public Discussion	**Case Number**	00000061

Additional Root Case Information

Subject	Include CA WoSign ECC Root

Technical Information about Root Certificate

O From Issuer Field	WoSign CA Limited	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	This ECC root will have internally-operated intermediate certificates that issue SSL, Code Signing, and Client certificates to individuals and organizations	**Verified?**	Verified
Root Certificate Download URL	http://www.wosign.com/root/ws_ecc.crt	**Verified?**	Verified
Valid From	2014 Nov 08	**Verified?**	Verified
Valid To	2044 Nov 08	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	ECC	**Verified?**	Verified
Signing Key Parameters	ECC P-384	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://root5evtest.wosign.com/	**Verified?**	Verified
CRL URL(s)	http://crls8.wosign.com/ca8.crl http://crls8.wosign.com/ca8-ssl4.crl CPS 7.8: CRL Next Update: 5 days	**Verified?**	Verified
OCSP URL(s)	http://ocsp8.wosign.com/ca8 http://ocsp8.wosign.com/ca8/ssl4	**Verified?**	Verified
Revocation Tested		**Verified?**	
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	1.3.6.1.4.1.36305.2	**Verified?**	Verified

EV Tested	// CN=CA WoSign ECC Root,O=WoSign CA Limited,C=CN "1.3.6.1.4.1.36305.2", "WoSign EV OID", SEC_OID_UNKNOWN, { 0x8B, 0x45, 0xDA, 0x1C, 0x06, 0xF7, 0x91, 0xEB, 0x0C, 0xAB, 0xF2, 0x6B, 0xE5, 0x88, 0xF5, 0xFB, 0x23, 0x16, 0x5C, 0x2E, 0x61, 0x4B, 0xF8, 0x85, 0x56, 0x2D, 0x0D, 0xCE, 0x50, 0xB2, 0x9B, 0x02 }, "MEYxCzAJBgNVBAYTAkNOMRowGAYDVQQKExFXb1NpZ24gQ0EgTGltaXRlZDEbMBkG" "A1UEAxMSQ0EgV29TaWduIEVDQyBSb290", "aEpYcIBr8I8C+vbe6LCQkA==", Success!	**Verified?**	Verified
Root Stores Included In		**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	D2:7A:D2:BE:ED:94:C0:A1:3C:C7:25:21:EA:5D:71:BE:81:19:F3:2B	**Verified?**	Verified
SHA-256 Fingerprint	8B:45:DA:1C:06:F7:91:EB:0C:AB:F2:6B:E5:88:F5:FB:23:16:5C:2E:61:4B:F8:85:56:2D:0D:CE:50:B2:9B:02	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	The plan is to have 10 internally-operated subCAs for 3 types of certificates: SSL Certificate, Code Signing Certificate and Client Certificate. 1. WoSign Class 4/3/2/1 EV/OV/IV/DV ECC SSL CA 2. WoSign Class 4/3/2 EV/OV/IV ECC Code Signing CA 3. WoSign Class 3/2/1 ECC Client CA Currently, one of the subCAs has been issued: WoSign Class 4 EV ECC SSL 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	External third parties may not cause the issuance of certificates in this CA hierarchy.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Document Repository (Chinese): http://www.wosign.com/policy/cps.htm	**Verified?**	Verified
CA Document Repository	http://www.wosign.com/policy/cps_e.htm	**Verified?**	Verified
CP Doc Language			
CP		**Verified?**	Not Applicable
CP Doc Language			
CPS	http://www.wosign.com/policy/wosign-policy-1-2-12.pdf	**Verified?**	Verified

Other Relevant Documents		**Verified?**	Not Applicable
Auditor Name	Ernst & Young (EY)	**Verified?**	Verified
Auditor Website	http://www.ey.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1843&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	2/28/2015	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1860&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	4/10/2015	**Verified?**	Verified
EV Audit	https://cert.webtrust.org/SealFile?seal=1842&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	2/28/2015	**Verified?**	Verified
BR Commitment to Comply	CPS section 1.2.	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2.1.2: Fully qualified domain names ... 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 - admin@domain.com - administrator@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 be the domain name registrar. If the WHOIS data contain an administrative email addresses, that may be offered as additional choice to the above mentioned electronic mail accounts. If the subscriber can't receive email from the above email account, he/she can choose to do the website control validation that the subscriber must upload a website control validation code file to the website root directory to finish the website control validation. CPS section 3.2.2.3 (Class 3): Domain and email control validation is performed as in Class 1. Domain control may also be established through verification of the WHOIS records and matching subscriber information.	**Verified?**	Verified

EV SSL Verification Procedures	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.	**Verified?**	Verified
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.	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.2.1.1: 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 and electronic mail message. CPS section 3.2.2.2 (Class 2): Email control validation is performed as in Class 1.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	According to section 3.1.1 of the CPS, the validation levels allowed for Code Signing certs are Class 2, Class 3, or Class 4/EV. Steps taken to verify the identity of the certificate subscriber and verify the organization are described in section 3.2.2 of the CPS, and steps taken to verify the authority of the certificate subscriber to act on behalf of the organization are described in section 3.2.4.	**Verified?**	Verified
Multi-Factor Authentication	CPS section 5.3. Client Certificate in USB Key.	**Verified?**	Verified
Network Security	CPS sections 5 and 6	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://www.wosign.com/english/root.htm	**Verified?**	Verified