1. Cross-signed CA Company Name: WoSign CA Limited

2. Corporate URL: http://www.wosign.com/
http://www.wosign.com/English/

3. CA certificate download URL:

http://crt.comodoca.com/CertificationAuthorityofWoSign_Object.crt
http://crt.comodoca.com/CertificationAuthorityofWoSign_Server.crt

4. URL to a test website whose SSL certificate chains up to this Sub-CA's certificate (if this Sub-CA is allowed to issue SSL certificates)

https://utn-wosign-xs-test.wosign.com

5. General CA hierarchy under the sub-CA.

There are 7 internally-operated subordinate CAs for this 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

6. Sub-CA CP/CPS Links

http://www.wosign.com/Policy/CPS_E.htm
http://www.wosign.com/Policy/wosign-policy-1_2_2.pdf

7. The section numbers and text (in English) in the CP/CPS that demonstrate that reasonable measures are taken to verify the ownership of the domain name and email address for end-entity certificates chaining up to the root, as per section 7 of our Mozilla CA certificate policy.

domain ownership/control:

3.2.2.1.2. Domain Names

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.
WoSign performs additional sanity and fraud prevention checks as outlined in section 3.1.6.
Wild card domain names like “*.domain.com" are not issued in the Class 1 level.
WoSign SSL certificate support IDN domain in Chinese and other languages, so Wosign makes a reasonable check for similar sounding and looking names to prevent possible abuse which is applied also to non-IDN names such as PAYPA1.COM, MICROSOFT.COM etc. and all IDN domain also need the domain ownership verification by system same as normal non-IDN domains. The validation may be valid for 30 days for the generation of certificates.

email address ownership/control:

3.2.2.1.1. Email Addresses

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.
The validation may be valid for 30 days for the generation of digital certificates.

digitally signing code objects -- entity submitting the certificate signing request is the same entity referenced in the certificate

3.2.2.2.1. Personal Identity

The verification process of personal identities of subscribers are performed manually. The WoSign CA validates without any reasonable doubt that the following details are correct:

- First and last name
- Residence, Address
- State or Region
- Country

The subscriber has to provide in a secure and reliable fashion one scanned or photographed identification papers in high quality and resolution. The documents must be valid in every respect and not be expired.

If the accuracy of the documents is in doubt as to the correctness of the details provided, WoSign may request the original documents and/or a copy of the original document confirmed, signed and stamped by the issuing authority or Latin notary via postal mail. Any document obtained physically may be scanned or photographed for archiving purpose at the premise of WoSign and shall be returned to the sender via registered postal mail.
WoSign may verify the correctness of the identity through payment transactions to its banking accounts by the subscriber. The transaction details must state the correct personal details of the subscriber.
Alternatively WoSign may use third party records to establish that a phone number is owned by the subscriber and by performing a verification call.

Email control validation is performed as in Class 1.
The validation may be valid for 350 days for the generation of digital certificates.

3.2.2.3.1. Organization

The verification process of organizations implies same level identity validation of the subscriber (responsible person) and are performed manually. WoSign validates without any reasonable doubt that the following details are correct:

- Registered organization name
- Address
- State or Region
- Country

The subscriber has to provide in a secure and reliable fashion supporting documentation. The documents must be valid in every respect and not be expired.
If the accuracy of the documents is in doubt as to the correctness of the details provided, WoSign may request the original documents and/or a copy of the original document confirmed, signed and stamped by the issuing authority via postal mail. Any document obtained physically may be scanned or photographed for archiving purpose at the premise of WoSign and shall be returned to the sender via registered postal mail.
WoSign may verify the correctness of the organization details through payment transactions to its banking accounts by the subscriber. The transaction details must state the correct organization details of the subscriber. Additionally WoSign obtains through third party records a phone number that is owned by the organization and by performing a verification call. During the verification call WoSign establishes the authority of the subscriber.

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.
The validation may be valid for 350 days for the generation of digital certificates.

8. Identify if the SSL certificates chaining up to the sub-CA are DV, OV, and/or EV.

The certificates issued from http://crt.comodoca.com/CertificationAuthorityofWoSign_Server.crt will include DV and OV SSL certificates.

In addition, the same CA will issue EV certificates but is contractually constrained from issuing EV SSL certificates including Comodo's EV policy OID. I.e. WoSign will use their own EV policy OID as set out in their CPS.

Review the CP/CPS for Potentially Problematic Practices. Provide further info when a potentially problematic practice is found.

Mozilla have reviewed the CPS for problematic practices.
https://bug851435.bugzilla.mozilla.org/attachment.cgi?id=812771

If the root CA audits do not include this sub-CA, then for this sub-CA provide a publishable statement or letter from an auditor that meets the requirements of sections 11, 12, 13, and 14 of Mozilla's CA Certificate Inclusion policy.

http://cert.webtrust.org/SealFile?seal=1443&file=pdf
http://cert.webtrust.org/SealFile?seal=1423&file=pdf