Information checklist for CAs applying for inclusion in Mozilla

* General information about the associated organization of the CA

1. Name
   - This is the name by which the CA is most commonly known, e.g., "GeoTrust"

     WoSign eCommerce Services Limited, DBA: WoSign
2. Website URL: www.wosign.com
3. Organizational type
   - Indicate whether the CA is operated by a private or public corporation, government agency, international organization, academic institution or consortium, NGO, etc. Note that in some cases the CA may be of a hybrid type, e.g., a corporation established by the government. For government CAs, the type of government should be noted, e.g., national, regional/state/provincial, or municipal.)

     A private corporation
4. Primary market / customer base
   - Which types of customers does the CA serve?

     The general public
   - Are there particular vertical market segments in which it operates?

     No. To all market segments.
   - Does the CA focus its activities on a particular country or other geographic region?

     No. But start from China market.
5. Impact to Mozilla Users

   1. Why does the CA need to have their root certificate directly included in Mozilla's products, rather than being signed by another CA's root certificate that is already included in NSS?

      Now, China have more than 500M Internet user and more than 3M website, up to 90% website have not deploy SSL certificate, this is a serious security problem for Microsoft customers in China;

      Currently, a few of foreign CAs like Symantec (VeriSign, GeoTrust, Thawte) to issue certificates for China customers by its reseller; the problems are:

      (1) Its certificates only support English that 90% China Internet users don't understand. It gives the chance for fraud websites. For example, the No.1 bank in China's English name is Industrial and Commercial Bank of China (ICBC), its website deployed VeriSign EV SSL that display this English name that 99% China Internet users don't understand; if it deploy WoSign EV SSL, it will display its Chinese name like: 中国工商银行 that all China Internet users can understand;

(2) Foreign CA's local service is provided by its reseller that just guide end user to install the certificate, the reseller don't have the enough technology to guide customer the other SSL related problem like disable SSL V2.0, and disable the Legacy Renegotiation protocol and disable 40bit/56bit Cipher Suites etc.

(3) The foreign CA's OCSP/CRL server connection has the long time latency, timeout problem, and sometime it can't connect since it don't setup OCSP server in China.

WoSign resell certificates from 2004 (as a GeoTrust, Thawte and VeriSign reseller), and became a SubCA of Comodo at 2006 that start to issue WoSign brand certificates to China market. And WoSign setup its own root CA at 2009 and start to issue certificates at 2011 under this root CA that cross signed with Startcom CA. We issued thousands certificates to China customers, WoSign SSL certificate is deployed in top 10 eCommerce websites in China, and for bank, telecom, enterprise etc., and most software developers in China choose WoSign certificate since it support 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.

WoSign will do the market promotion in China after we join the Program, to educate the market for PKI technology, to popularize the PKI technology in enterprise IT system and ecommerce websites. We are confident that we can provide broad value to Mozilla customers in China and worldwide.

- Does this CA have root certificates included in any other major browsers? If yes, which? If no, why not?
  NO, it is applying with Microsoft, Apple in the same time.

- Describe the types of Mozilla users who are likely to encounter your root certificate as relying parties while web browsing (HTTPS servers doing SSL), sending/receiving email to their own MTA (SMTPS, IMAPS servers doing SSL), sending/receiving S/MIME email (S/MIME email certs), etc.

Server Authentication	**EKU=1.3.6.1.5.5.7.3.1**
Client Authentication	**EKU=1.3.6.1.5.5.7.3.2**
Secure Email	**EKU=1.3.6.1.5.5.7.3.4**
Code Signing	**EKU=1.3.6.1.5.5.7.3.3**

Time stamping **EKU=1.3.6.1.5.5.7.3.8**

- Mozilla CA certificate policy:
  - We will determine which CA certificates are included in software products distributed through mozilla.org, based on the benefits and risks of such inclusion to typical users of those products.
  - We require that all CAs whose certificates are distributed with our software product ... provide some service relevant to typical users of our software products

6. CA Contact Information
   - CA Email Alias: An email alias is being requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization.
     ca@wosign.com
   - CA Phone Number: A main phone number from which Mozilla can reach the organization responsible for root certificates for the CA.
     +86-755-26027858, 86008688
   - Title / Department: If Mozilla needed to call your main phone number, what Title/Department should the Mozilla representative ask for?
     Mr. Richard Wang, CTO

* Technical information about each root certificate

The information listed in this section must be provided for each root CA whose certificate is to be included in Mozilla, or whose metadata is to be modified.

** WoSign Root CA1:

1. Certificate Name: **Certification Authority of WoSign**
   - This is the "friendly name" to be used when displaying information about the root, e.g., "GeoTrust Global CA". It is typically identical to or a variant of the CN found within the Subject attribute of the root CA certificate itself.
2. Certificate Issuer Field
   - The Organization Name and CN in the Issuer must have sufficient information about the CA Organization.
     CN=Certification Authority of WoSign
     O=WoSign eCommerce Services Limited
     C=CN

3. Certificate Summary
   - A summary about this root certificate, its purpose, and the types of certificates that are issued under it.
     To provide SSL certificates for Website; Code signing certificates for code publisher and Client certificates for individuals and organizations etc.

This CA is for China market. China needs a local commercial CA to provide local CA services with all certificates supporting Chinese and IDN domains.

4. Root Certificate URL
    - A public URL through which the CA certificate can be directly downloaded.

      http://www.wosign.com/Root/ca1.crt

5. SHA1 fingerprint:

   33:A4:D8:BC:38:60:8E:F5:2E:F0:E2:8A:35:09:1E:92:50:90:7F:B9

6. Valid from (YYYY-MM-DD): **2009-08-08**
    - The date from which the root CA certificate is valid.
7. Valid to (YYYY-MM-DD): **2039-08-08**
    - The date until which the root CA certificate is valid.
8. Certificate Version (should be 3): **V3**
    - The X.509 certificate version
9. Certificate Signature Algorithm: **SHA1 with RSA Encryption**
10. Signing key parameters: **4096 bits**
    - For RSA keys, the modulus length, for example, 2048 or 4096 bits.
    - For ECC keys, the named curve, for example, NIST Curve P-256, P-384, or P-512.
11. Test website URL -- if you are requesting to enable the Websites (SSL/TLS) trust bit
    - URL to a website whose SSL cert chains up to this root. Note that this can be a test site.

      https://www.wosign.com
        - Intermediate CA certificates are expected to be distributed to the certificate subjects (the holders of the private keys) together with the subjects' own certificates. Those subject parties (e.g. SSL servers) are then expected to send out the intermediate CA certificates together with their own certificates whenever they are asked to send out their certificates. That is required by SSL/TLS.
        - Certificate authorities MUST advise their subscribers that all intermediate certificates should be installed in the servers containing the dependent subscriber certificates.
12. Example certificates
    - If this root does not issue certificates for SSL, then provide example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s).
13. Certificate Revocation Lists (CRLs)
    - URL(s) at which the CRL(s) may be obtained -- for end-entity certs and for intermediate CAs.

      http://crls.wosign.com/ca.crl
      http://crls.wosign.com/server-4.crl
      http://crls.wosign.com/server-3.crl
      http://crls.wosign.com/server-1.crl
      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

- The value that next Update is set to in the CRLs for end-entity certificates.
  48 hours
- The sections of your CP/CPS documentation that state the requirements about frequency of updating 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.
- Note the CA/Browser Forum's EV guidelines: CRLs MUST be updated and reissued at least every seven days, and the nextUpdate field value SHALL NOT be more ten days
- You must test your CRLs by importing them into the Firefox browser.
  - Error Codes:
    - ffffe095, is equivalent to -8043, SEC_ERROR_CRL_UNKNOWN_CRITICAL_EXTENSION Resolution: See Potentially Problematic Practice CRL with Critical CIDP Extension
    - ffffe009 is equivalent to -8183, “Security library: improperly formatted DER-encoded message.” It means that the reply contained anything other than a valid DER-encoded CRL. Typical Resolution: Change encoding from PEM to DER.

      Test is ok.

14. OCSP (OCSP is required for EV enablement)
    - The OCSP URI that is in the AIA of your subscriber certificates.
      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

    - The maximum time elapsing from the revocation of an end entity or CA certificate until OCSP responders are updated to reflect that revocation. The current OCSP responders are updated at least every 60 minutes.
      3 hours
    - The sections of your CP/CPS specifying availability and update requirements for the OCSP service.

        - CA/Browser Forum's EV Guidelines Section 26(b): “If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days.”
          The current CRLs are reloaded at least every 60 minutes.

    - You must test that your OCSP service is compatible with the Firefox browser.
        - See: https://wiki.mozilla.org/CA:Recommended_Practices#OCSP
        - OCSP responders should be set up to listen on a standard port (e.g. port 80), because firewalls may block ports other than 80/443.
          Test is ok.

    - If you are requesting to enable EV, then you must also perform the PSM EV Testing to ensure that OCSP works correctly up the chain.
        - For more information about EV see EV Revocation Checking and EV Testing Details.
          Test is OK.

15. Requested Trust Bits
    - State which of the three trust bits you are requesting to be enabled for this root. One or more of:
        - Websites (SSL/TLS)
        - Email (S/MIME)
        - Code Signing
          All 3 bits.
    - Mozilla’s standpoint is that we should operate the root program in terms of minimizing risk. One way that we can minimize risk is by not enabling more trust bits than CAs absolutely require.
16. SSL Validation Type
    - Indicate the levels of SSL validation that are used for certificates within this root's hierarchy. One or more of:
        - DV -- The ownership of the domain name is verified, but the identity/organization of the subscriber is not verified.
        - OV -- In addition to verifying the domain ownership, you also validate the organization to be listed in the O field - making sure public record and government resources can verify the address, existence, and good legal standing of the organization itself. Verifying that the whois listed address matches the verified address, and any other additional checks that a given CA lists in its CPS.
        - EV - Verification meets the requirements of the CA/Browser Forum CA/Browser Forum's EV Guidelines
          All 3 level: DV/OV/EV.

17. If EV certificates are issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.

    1.3.6.1.4.1.36305.2

** WoSign Root CA2:

1. Certificate Name: **CA WoSign**
    - This is the "friendly name" to be used when displaying information about the root, e.g., "GeoTrust Global CA". It is typically identical to or a variant of the CN found within the Subject attribute of the root CA certificate itself.
2. Certificate Issuer Field
    - The Organization Name and CN in the Issuer must have sufficient information about the CA Organization.
      CN=CA WoSign
      O=WoSign eCommerce Services Limited
      C=US

3. Certificate Summary
    - A summary about this root certificate, its purpose, and the types of certificates that are issued under it.
      To provide SSL certificates for Website; Code signing certificates for code publisher and Client certificates for individuals and organizations etc.
      This CA is for international market.
4. Root Certificate URL
    - A public URL through which the CA certificate can be directly downloaded.

      http://www.wosign.com/Root/ws_ca2.crt

5. SHA1 fingerprint:

   AF:F5:F5:BD:B7:CF:2B:6D:0C:FB:2D:6A:2A:95:9A:07:CE:34:33:8B

6. Valid from (YYYY-MM-DD): **2009-08-08**
    - The date from which the root CA certificate is valid.
7. Valid to (YYYY-MM-DD): **2039-08-08**
    - The date until which the root CA certificate is valid.
8. Certificate Version (should be 3): **V3**
    - The X.509 certificate version
9. Certificate Signature Algorithm: **SHA1 with RSA Encryption**
10. Signing key parameters: **4096 bits**
    - For RSA keys, the modulus length, for example, 2048 or 4096 bits.
    - For ECC keys, the named curve, for example, NIST Curve P-256, P-384, or P-512.
11. Test website URL -- if you are requesting to enable the Websites (SSL/TLS) trust bit
    - URL to a website whose SSL cert chains up to this root. Note that this can be a test site.
      To be provided

- Intermediate CA certificates are expected to be distributed to the certificate subjects (the holders of the private keys) together with the subjects' own certificates. Those subject parties (e.g. SSL servers) are then expected to send out the intermediate CA certificates together with their own certificates whenever they are asked to send out their certificates. That is required by SSL/TLS.
- Certificate authorities MUST advise their subscribers that all intermediate certificates should be installed in the servers containing the dependent subscriber certificates.

12. Example certificates
    - If this root does not issue certificates for SSL, then provide example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s).
13. Certificate Revocation Lists (CRLs)
    - URL(s) at which the CRL(s) may be obtained -- for end-entity certs and for intermediate CAs.
      http://uscrls.wosign.com/ca.crl
      http://uscrls.wosign.com/server-4.crl
      http://uscrls.wosign.com/server-3.crl
      http://uscrls.wosign.com/server-1.crl
      http://uscrls.wosign.com/client-1.crl
      http://uscrls.wosign.com/client-2.crl
      http://uscrls.wosign.com/client-3.crl
      http://uscrls.wosign.com/code-3.crl

    - The value that next Update is set to in the CRLs for end-entity certificates.
      48 hours
    - The sections of your CP/CPS documentation that state the requirements about frequency of updating 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.
    - Note the CA/Browser Forum's EV guidelines: CRLs MUST be updated and reissued at least every seven days, and the nextUpdate field value SHALL NOT be more ten days
    - You must test your CRLs by importing them into the Firefox browser.
      - Error Codes:
        - ffffe095, is equivalent to -8043, SEC_ERROR_CRL_UNKNOWN_CRITICAL_EXTENSION Resolution: See Potentially Problematic Practice CRL with Critical CIDP Extension
        - ffffe009 is equivalent to -8183, “Security library: improperly formatted DER-encoded message.” It means that the reply

contained anything other than a valid DER-encoded CRL.
Typical Resolution: Change encoding from PEM to DER.

Test is ok.

14. OCSP (OCSP is required for EV enablement)
    - The OCSP URI that is in the AIA of your subscriber certificates.
      http://usocsp.wosign.com/ca
      http://usocsp.wosign.com/class4/server/ca
      http://usocsp.wosign.com/class3/server/ca
      http://usocsp.wosign.com/class1/server/ca
      http://usocsp.wosign.com/class1/client/ca
      http://usocsp.wosign.com/class2/client/ca
      http://usocsp.wosign.com/class3/client/ca
      http://usocsp.wosign.com/class3/code/ca

    - The maximum time elapsing from the revocation of an end entity or CA certificate until OCSP responders are updated to reflect that revocation.
      The current OCSP responders are updated at least every 60 minutes.
      3 hours
    - The sections of your CP/CPS specifying availability and update requirements for the OCSP service.
      - CA/Browser Forum's EV Guidelines Section 26(b): "If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days."
        The current CRLs are reloaded at least every 60 minutes.

    - You must test that your OCSP service is compatible with the Firefox browser.
      - See: https://wiki.mozilla.org/CA:Recommended_Practices#OCSP
      - OCSP responders should be set up to listen on a standard port (e.g. port 80), because firewalls may block ports other than 80/443.
        Test is ok.

    - If you are requesting to enable EV, then you must also perform the PSM EV Testing to ensure that OCSP works correctly up the chain.
      - For more information about EV see EV Revocation Checking and EV Testing Details.
        Test is OK.

15. Requested Trust Bits
    - State which of the three trust bits you are requesting to be enabled for this root.
      One or more of:
      - Websites (SSL/TLS)

        - Email (S/MIME)
        - Code Signing

          All 3 bits.
    - Mozilla's standpoint is that we should operate the root program in terms of minimizing risk. One way that we can minimize risk is by not enabling more trust bits than CAs absolutely require.
16. SSL Validation Type
    - Indicate the levels of SSL validation that are used for certificates within this root's hierarchy. One or more of:
        - DV -- The ownership of the domain name is verified, but the identity/organization of the subscriber is not verified.
        - OV -- In addition to verifying the domain ownership, you also validate the organization to be listed in the O field - making sure public record and government resources can verify the address, existence, and good legal standing of the organization itself. Verifying that the whois listed address matches the verified address, and any other additional checks that a given CA lists in its CPS.
        - EV - Verification meets the requirements of the CA/Browser Forum CA/Browser Forum's EV Guidelines

          All 3 level: DV/OV/EV.
17. If EV certificates are issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.

    1.3.6.1.4.1.36305.2

* CA Hierarchy information for each root certificate

The information listed in this section must be provided for each root certificate to be included in Mozilla, or whose metadata is to be modified.

If Mozilla accepts and includes your root certificate, then we have to assume that we also accept any of your future sub-CAs and their sub-CAs. Therefore, the selection criteria for your sub-CAs and their sub-CAs will be a critical decision factor. As well as the documentation and auditing of operations requirements that you place on your sub-CAs and their sub-CAs.

1. CA Hierarchy
    - A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate.
        - List and/or describe all of the subordinate CAs that are signed by this root.

          There are 7 subordinate CAs for this root CA:

          (1) WoSign Class 4 EV Server CA: for Class 4 EV SSL certificate

(2) WoSign Class 3 OV Server CA: for Class 3 OV SSL certificate
(3) WoSign Class 1 DV Server CA: for Class 1 DV SSL certificate
(4) WoSign Class 3 Code Signing CA: for Class 3 Code Signing certificate
(5) WoSign Class 1 Client CA: for Class 1 Client Certificate
(6) WoSign Class 2 Client CA: for Class 2 Client Certificate
(7) WoSign Class 3 Client CA: for Class 3 Client Certificate

- Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.
  All above 7 Sub CAs are internally-operated.
  - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do *not* require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements.
    No such Sub CA.

2. Sub CAs Operated by 3rd Parties
   - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist
     NO.
   - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.
     NO.
3. Cross-Signing
   - List all other root certificates for which this root certificate has issued cross-signing certificates.
     NO.
   - List all other root certificates that have issued cross-signing certificates for this root certificate.
     Startcom CA issued cross-signing certificate for this root CA, detail:
     CN = StartCom Certification Authority
     Thumbprint: 3e 2b f7 f2 03 1b 96 f3 8c e6 c4 d8 a8 5d 3e 2d 58 47 6a 0f
   - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.
     Yes, it is already included.
4. Technical Constraints or Audits of Third-Party Issuers

- For each external third party (CAs and RAs) that issues certificates or can directly cause the issuance of certificates within the hierarchy of the root certificate(s) that you wish to include in Mozilla products, either:
  - Implement technical controls to restrict issuance to a specific set of domain names which you have confirmed that the third party has registered or has been authorized to act for (e.g. RFC5280 x509 dNSName name constraints, marked critical)
  - OR
  - Provide the name and url of the unconstrained third party along with links to their corresponding Certificate Policy and/or Certification Practice Statement and provide attestation of their conformance to the stated verification requirements and other operational criteria by a competent independent party or parties with access to details of the subordinate CA's internal operations.

    NO.

* Verification Policies and Practices

We rely on publicly available documentation and audits of those documented processes to ascertain that the CA takes reasonable measures to confirm the identity and authority of the individual and/or organization of the certificate subscriber.

If the CP/CPS documents are not in English, then the portions of those documents pertaining to verification of the certificate subscriber **must be translated into English**. For all of the items listed below, provide both a pointer to the original document (and section or page number of the relevant text) as well as the translated text.

1. Documentation: CP, CPS, and Relying Party Agreements
   - The publicly accessible URLs to the document repository and the published document(s) describing how certificates are issued within the hierarchy rooted at this root, as well as other practices associated with the root CA and other CAs in the hierarchy, including in particular the Certification Practice Statement(s) (CPS) and related documents.

     http://www.wosign.com/policy/WoSign-Policy-1_1.pdf

   - The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3.

     CPS: Page 2 "1.3.1.2. Commitment to comply with applicable standards**", will update to v1.2 "Comply BR" clearly.**
2. Audits
   - The publicly accessible URLs to the published document(s) relating to independent audit(s) of the root CA and any CAs within the hierarchy rooted at the root. For example, for WebTrust for CAs audits this would be the "audit report and management assertions" document available from the webtrust.org

site or elsewhere.
https://cert.webtrust.org/ViewSeal?id=1443
For EV readiness, no seal is available, but we have the report.

- We need a publishable statement or letter from an auditor (who meets the requirements of the Mozilla CA Certificate Policy) that states that they have reviewed the practices as outlined in the CP/CPS for these roots, and that the CA does indeed follow these practices and meets the requirements of one of:
  - ETSI TS 101 456
  - ETSI TS 102 042
  - WebTrust Principles and Criteria for Certification Authorities
    WebTrust by Ernst & Young

- Audits performed after January 2013 need to include verification of compliance with the CA/Browser Forum Baseline Requirements if SSL certificates may be issued within the CA hierarchy, and the audit statement shall indicate the results.
  N/A
- When audit statements are provided by the company requesting CA inclusion rather than having an audit report posted on the website such as cert.webtrust.org, the Mozilla process requires doing an independent verification of the authenticity of audit statements that have been provided. Provide the website and email address for the company that provided the audit statement.
  - If the information is available from the auditor's (or other third-party's) web site or from another authoritative web site (for example, webtrust.org for WebTrust reports), please provide the URL where the information can be found.
  - If you provide the information yourself (e.g., it is hosted on your own web site), please provide us with contact information for the auditor (or other third party).
  - Otherwise please ask the auditor (or other third party) to contact us directly and provide us the audit report(s) or other information.
    N/A
- The audit should not be more than a year old. If it is, then provide an estimate of when the updated audit report will be available. While ETSI Certificates may be valid for 3 years, it is our expectation that there is an annual renewal/review process for the ETSI Certificate to remain valid.
  N/A
- Renewed root certificates also need to be included in audits. If the root certificate was created after the most recent audit, then provide an estimate of when the new audit report (that includes the operations of the new root) will be available.
  N/A

- Government CAs
  - According to section 9 of Mozilla's CA Certificate Inclusion Policy, the audit must be performed according to criteria that is equivalent to one (or more) of ETSI TS 101 456, ETSI TS 102 042, or WebTrust CA. The government's auditing agency should provide a statement about which of these their government criteria is equivalent to.
  - According to sections 10 and 11 of Mozilla's CA Certificate Inclusion Policy, it is acceptable for a government auditing organization to perform the audit of the government's CA organization. It must be clear that the CA organization does not audit itself.

    N/A

3. SSL Verification Procedures
   - If you are requesting to enable the Websites (SSL/TLS) trust bit...
     - URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying that the domain referenced in an SSL cert is owned/controlled by the subscriber.
       - Recommended Practices for Verifying Domain Name Ownership

         CPS: Page 12, 3.2.2.1.2
     - If a challenge-response mechanism via email is used to confirm the ownership/control of the domain name, then provide the list of email addresses that are used for verification.
       - Potentially Problematic Practices in regards to Email Address Prefixes -- The list that the CA uses must either match or be a subset of the list in this wiki page.

         4 Emails: webmaster@, hostmaster@, postmaster@ and Whois Admin email.
     - Confirm that you have automatic blocks in place for high-profile domain names (including those targeted in the DigiNotar and Comodo attacks in 2011).
       - Specify the procedure for additional verification of a certificate request that is blocked.

         Yes. All famous brand domain application will flagged to wait for additional review by CVO(Chief Validation Officer)
     - If OV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying the identity, existence, and authority of the organization to request the certificate.
       - There should be a description of the types of resources that are used to confirm the authenticity of the information provided by the certificate subscriber, what data is retrieved from public resources, and how that data is used for verification of the

entity referenced in the certificate.

CPS: Page 14, 3.2.2.3

- If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate.
  - The EV verification documentation must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations.

CPS: Page 15, 3.2.2.4

4. Email Address Verification Procedures
   - If you are requesting to enable the Email (S/MIME) trust bit...
     - URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying that the email address to be included in the certificate is owned/controlled by the certificate subscriber.
     - Recommended Practices for Verifying Email Address
       - Note that per the Mozilla policy this verification must be done *in addition to* any verification of the subscriber's legal identity.

CPS: Page 12, 3.2.2.1.1

     - If subscriber identity verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying the identity and authority of the certificate subscriber.

CPS: Page 13, 3.2.2.2

5. Code Signing Subscriber Verification Procedures
   - If you are requesting to enable the Code Signing trust bit...
     - URLs and section/page number information pointing directly to the sections of the CP/CPS documents that describe the procedures for verifying the certificate subscriber's identity and authority, and the organization's identity and existence.
       - Recommended Practices for Verifying Identity of Code Signing Certificate Subscriber

CPS: Page 14, 3.2.2.3

6. Multi-factor Authentication
   - Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance or specify the technical controls that are implemented by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses.
     - For each account that can access the certificate issuance system, do you have the log-in procedure require something in addition to

username/password?
Yes.

- Specify the form factor that you use. Examples of multi-factor authentication include smartcards, client certificates, one-time-passwords, and hardware tokens.
  Client Certificate in USB Key.
- This must apply to all accounts that can cause the approval and/or issuance of end-entity certificates, including your RAs and sub-CAs, unless there are technical controls that are implemented and controlled by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses.
  Yes.
- If technical controls are used instead of multi-factor auth for any accounts, then specify what those technical controls are.
  N/A

7. Network Security
   - CAs must maintain current best practices for network security, and have qualified network security audits performed on a regular basis. The CA/Browser Forum has published a document called Network and Certificate System Security Requirements which should be used as guidance for protecting network and supporting systems.
   - Confirm that you have done the following, and will do the following on a regular basis:
     - Maintain network security controls that at minimum meet the Network and Certificate System Security Requirements.
       Yes.
     - Check for mis-issuance of certificates, especially for high-profile domains.
       Yes.
     - Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness.
       Yes.
     - Ensure Intrusion Detection System and other monitoring software is up-to-date.
       Yes.
     - Confirm that you will be able to shut down certificate issuance quickly if you are alerted of intrusion.
       Yes.

* Response to Mozilla's CA Recommended Practices

Review Mozilla's CA Recommended Practices. If your practices differ from any of these recommended practices, then describe those differences and explain how the

concern(s) are addressed.
No.

* Response to Mozilla's list of Potentially Problematic Practices

Review Mozilla's list of Potentially Problematic Practices. For each one, state if it is or is not applicable. For the ones that are applicable, provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that are relevant, and explain how you address the concern(s).

1. Long-lived DV certificates: No
2. Wildcard DV SSL certificates: No
3. Email Address Prefixes for DV Certs: No
4. Delegation of Domain / Email validation to third parties: No
5. Issuing end entity certificates directly from roots: No
6. Allowing external entities to operate subordinate CAs : No
7. Distributing generated private keys in PKCS#12 files: No
8. Certificates referencing hostnames or private IP addresses : No
9. Issuing SSL Certificates for Internal Domains : No
10. OCSP Responses signed by a certificate under a different root : No
11. CRL with critical CIDP Extension : No
12. Generic names for CAs : No
13. Lack of Communication With End Users : No