General information about the associated organization of the CA

1. Name
    - **Solutions Notarius Inc.**
2. URL to company website : **https://notarius.com**
3. Organizational type - One or more of the following choices that most accurately represents your CA's organization: Private Corporation, Public Corporation, Government Agency, Commercial Organization, International Organization, Non-Profit Organization, Academic Institution, Consortium, NGO.
    - **Private Corporation**
4. Primary market / customer base
    - Which types of customers does the CA serve? **Professionals, Governments, and legal customers. (https://notarius.com/en/industry/)**
    - Are there particular vertical market segments in which it operates?
    - Does the CA focus its activities on a particular country or other geographic region? **Mostly North American customers, but our solution is available worldwide.**
5. Impact to Mozilla Users
    - If your CA will only issue certificates within your organization or for a small number of websites, then rather than including your root certificate in NSS, please consider having your CA hierarchy cross-signed by an already-included CA. If your CA will be issuing certificates to the public or to a large number of websites, then please respond to the following questions. : **CA will be issuing certificates to the public.**
    - 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**? Our CA must be included directly in Mozilla's product. We issue certificate for several years and we control certificate generation/recover/revocation on the client side. It is impossible to get our CA signed by another CA, for 3 reasons: Our client put their trust in our CA and our CP, not on any other CA; It will be impossible to deploy on all our customers new chain of trust; Our current certification, ISO27001 and Webtrust for CA, will not allow to get our offline Root get signed by another CA.**
    - Does this CA have root certificates included in any other major browsers? If yes, which? If no, why not? **We are included in Microsoft Trusted Root Program and Adobe Trusted Root Program.**
    - 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. : **sending/receiving S/MIME email, Validation of PDF signed documents, User certificate authentication.**

- 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.

CA Primary Point of Contact (POC)

A CA may have more than one person filling the role of Primary Point of Contact (POC), and may use a contractor as one of the POCs. The CA must have one or more people within the CA's organization who jointly have authority to speak on behalf of the CA, and to direct whatever changes the review process or Mozilla's CA Communications require. At least one of the CA's POCs should also be in a position to make commitments for the CA and be held accountable by the CA.

The POCs will:

- Provide annual updates of CP/CPS documents, audit statements, and test websites.
- Respond to CA Communications
- Input and maintain the CA's data in the Common CA Database (CCADB)
- Inform Mozilla when there is a change in the organization, ownership, CA policies, or in the POCs that Mozilla should be aware of, as per
    - Common CCADB Policy
    - Mozilla's Root Store Policy
- Provide Mozilla with updated contact information if a new person becomes a POC.

Required contact information:

- Direct E-mail address, full name (first and last name), and phone number to a specific individual within the CA (must be one of the POCs).
    - **Alexandre Provost, IT Team Leader**
      alexandre.provost@notarius.com
      1-514-281-1577, x1226
    - **Patrick Drolet, VP Operations**
      Patrick.drolet@notarius.com
      1-514-281-1577, x1236

- 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. Mozilla CA Communications will be sent to both the POC direct email address(es) and the email alias.
    - **officers@notarius.com**
- CA Phone Number: A main phone number from which Mozilla can reach the organization responsible for root certificates for the CA.
    - **1-514-281-6311 – Support and Service**
- Title / Department: If Mozilla needed to call your main phone number, what Title/Department should the Mozilla representative ask for?
    - **IT Department, ask for Team Leader or Officer Department, ask for an Officer to help you.**

If the CA uses a contractor as an additional POC, then someone at the CA must be CC'd on the root inclusion Bugzilla bug, CA Communications, and the CA's responses to CA Communications.

- An individual within the CA must also get a Bugzilla account and comment in the bug to say that they will be a POC for the CA, and that the contractor has indeed been hired by the CA to act as one of the POCs. **There is no contractor imply in our CA structure.**

To ensure that the POC(s) has the authority to perform the tasks listed above, a representative of Mozilla will do the following.

1. Use the CA's website, to confirm that the domain in the email address of at least one of the POCs is owned by the CA (e.g. @CAname.com). **@notarius.com**
2. Use the CA's website to contact a person at the CA to confirm that at least one of the POCs that has been provided does indeed have the authority to perform the responsibilities listed above on behalf of the CA. **http://notarius.com/en/contact**
3. If a contractor is also used as a POC, then contact the POC that was previously verified to confirm that the CA has indeed enlisted the help of the contractor. **No contractor.**

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.

1. Certificate Name
    - 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. **Notarius Root Certificate Authority**
2. Certificate Issuer Field

- The Organization Name and CN in the Issuer must have sufficient information about the CA Organization.

  CN = Notarius Root Certificate Authority
  O = Notarius Inc
  C = CA

3. Certificate Summary

   - A summary about this root certificate, it's purpose, and the types of certificates that are issued under it.

     Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing

4. Root Certificate URL

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

     You will find a direct CA certificate download here :

     https://notarius.com/en/certification-policy/

5. SHA1 fingerprint

   1f 3f 14 86 b5 31 88 28 02 e8 7b 62 4d 42 02 95 a0 fc 72 1a

6. Valid from (YYYY-MM-DD)

   - The date from which the root CA certificate is valid.

     2014-12-17

7. Valid to (YYYY-MM-DD)

   - The date until which the root CA certificate is valid.

     2034-12-17

8. Certificate Version (should be 3)

   - The X.509 certificate version

     It is a certificate V3.

9. Certificate Signature Algorithm

   SHA256RSA

10. Signing key parameters

    - For RSA keys, the modulus length, for example, 2048 or 4096 bits.

      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.

      Not applicable. We are not issuing ssl certificate.

    - Please provide the 3 URLs to the test websites as described in Section 2.2 of the BRs: "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired

      Not applicable. We are not issuing ssl certificate.

    - Make sure you test it yourself in Firefox first, by doing the following:

      1. Create a new Firefox Profile for testing, as described in Mozilla's knowledge base articles: Profile Manager and Creating a new Firefox Profile.
      2. Import the root certificate as described here.
      3. Set OCSP hard fail as described here.
      4. Clear browser history
      5. Browse to the test website.
      6. Open the Web Console to check for any warnings (e.g. SHA-1, etc.) that should be addressed.

      - 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.

      Not applicable. We are not issuing ssl certificate.

- 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).

    See document annexed : Bug 1431811 – Mozilla application -Certificate Example.docx

- Certificate Revocation Lists (CRLs)

- URL(s) at which the CRL(s) may be obtained -- for end-entity certs and for intermediate CAs.

  http://crl.notarius.com/notarius_root_ca/crl/crl_roota1.crl

  http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl

  http://crl1.notarius.com/crl1-ca2/crl/notarius_certificate_authority_2_crlfull.crl

- The value that nextUpdate is set to in the CRLs for end-entity certificates.

  48h

- The sections of your CP/CPS documentation that state the requirements about frequency of updating CRL.

  http://notarius.com/wp-content/uploads/2018/01/Notarius-PKI-Certificate-Policy.pdf, section 2.3 - Time or Frequency of Publication

- 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

  We respect this guideline.

- OCSP (OCSP is required for the SSL trust bit to be enabled)
  - The OCSP URI that is in the AIA of your subscriber certificates.

    http://ocsp1.notarius.com/ocsp1-ca1

    http://ocsp1.notarius.com/ocsp1-ca2

  - The maximum time elapsing from the revocation of an end entity or CA certificate until OCSP responders are updated to reflect that revocation.

    Maximum 5 minutes

    http://notarius.com/wp-content/uploads/2018/01/Notarius-PKI-Certificate-Policy.pdf , section 4.5.4.1.

  - 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 OCSP have a maximum expiration time of 2 days, and update at least every 2h. We respect this guideline.

http://notarius.com/wp-content/uploads/2018/01/Notarius-PKI-Certificate-Policy.pdf , section 7.3

- You must test that your OCSP service is compatible with the Firefox browser.
  - See: https://wiki.mozilla.org/CA/Required_or_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.

    We are not issuing SSL Certificate, then it is more complicated to test our OCSP with Firefox. As describe in our CP/CPS (Section 7.3), our OCSP in adheres to the RFC 6960 standard. Our OCSP listen on port 80.

- Test!!!
  - ~~If requesting to enable the Websites (SSL/TLS) trust bit, then you must perform all of the following tests~~
    - ~~Revocation: Browse to https://certificate.revocationcheck.com/ and enter the Test Website URL. Make sure there are no errors listed in the output.~~
      - ~~If certificate.revocationcheck.com does not know about the root cert, then use the 'Certificate Upload' tab to directly input the PEM for the certificates.~~
    - ~~The CA MUST check that they are not issuing certificates that violate any of the CA/Browser Forum Baseline Requirements (BRs).~~
    - ~~Mozilla WILL check that the CA is not issuing certificates that violate any of the BRs by performing the following tests.~~
      - ~~Browse to https://crt.sh/~~
      - ~~Enter the SHA-1 or SHA-256 Fingerprint for the root certificate. Then click on the 'Search' button.~~
      - ~~When the certificate information is shown, along the left column under Certificate, click on the "Run cablint" and "Run x509lint" links. Each of these will add a row to the table, showing the test results.~~
      - ~~All errors must be resolved/fixed. Warnings should also be either resolved or explained.~~
    - ~~Alternatively, you may use the test code directly via Github:~~
      - ~~BR Lint Test: https://github.com/awslabs/certlint~~
      - ~~X.509 Lint Test: https://github.com/kroeckx/x509lint~~

- ~~All errors must be resolved/fixed. Warnings should also be either resolved or explained.~~

- ~~Test Errors - Meaning and recommended solutions to errors that CAs have run into while doing the tests listed above.~~

- ~~If you are requesting to enable EV treatment, then you must also perform the PSM EV Testing~~

- ~~You must provide successful output from the EV Checking Tool.~~

- Requested Trust Bits

  - State which of the two trust bits you are requesting to be enabled for this root. One or more of:

    - Websites (SSL/TLS)

    - Email (S/MIME)

    We are requesting the email (S/mime) bits. Email signature is not a product we are offering, we are issuing user certificates mainly for PDF signatures and validation. Your email bits is the most related trust bit you propose.

    https://notarius.com/en/what-we-do/

  - 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.

- ~~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~~

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

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 is signed by this Root.

          Notarius Certificate Authority : Subordinate CA of Notarius Root Certificate Authority. This subordinate is currently included in the Adobe Approved Trust List, and every user certificate issue by this subordinate CA are AATL approved in Adobe Software. Every certificate issue by this subordinate CA must be generated on Crypto Token.

          Notarius Certificate Authority 2 : Subordinate CA of Notarius Root Certificate Authority. User certificate issue by this subordinate CA is recognized by Microsoft Trust Store, since our Root CA is also trusted by Microsoft Trusted Root Program. User certificate issue by this subordinate is generated on software crypto-vault.

        - 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.

            - 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.

          Root CA and all Subordinate CA are operated by Solutions Notarius. Under no circumstances, a third party is involved.

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

- 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.

  Not applicable.

3. Cross-Signing

   - List all other root certificates for which this root certificate has issued cross-signing certificates.
   - List all other root certificates that have issued cross-signing certificates for this root certificate.
   - 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.

     There is no cross-signing relationships between any of our Root CA or Subordinate CA with other CA.

4. Technical Constraints or Audits of Third-Party Issuers.

   - As per section 5.3 of Mozilla's Root Store Policy, provide the required data for all of your non-technically-constrained subordinate CA certificates that chain up to certificates in Mozilla's CA program. This data may be provided as follows:
     - Already-included CAs may provide this information directly in the CCADB.
     - If you need to use the mozilla.org Bugzilla system to provide this information, then file the bug against the "CA Certificate Root Program" component of the "NSS" product. (https://bugzilla.mozilla.org/enter_bug.cgi?product=NSS&component=CA%20Certificate%20Root Program)

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 CP/CPS documents that are relevant to the root inclusion request **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.

- The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per section 2.2 in BRs.
- CP/CPS Documents will be reviewed, and must contain sufficient information for Mozilla and the CA Community to evaluate the CA's processes in regards to Mozilla's policies and the CA/Browser Forum's Baseline Requirements.
    - English translations must be provided for the relevant CP/CPS documents, and must match the current version of the CP/CPS documents.

    You will find the Certificate Pratice (CP) of Notarius Root Certificate Authority and his Subordinate CA on our website.

    https://notarius.com/en/certification-policy/

    http://notarius.com/wp-content/uploads/2018/01/Notarius-PKI-Certificate-Policy.pdf

    Regarding the CPS, this document is confidential and cannot be uploaded in Bugzilla. If you feel that our CP is incomplete, I will ask you to contact me directly and we will take arrangement to allow you to consult this document.

2. Audits

- The publicly accessible URLs to the published document(s) relating to an 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.

    Audit report and management assertions document available with our Webtrust Seal : https://cert.webtrust.org/ViewSeal?id=2240 (april 2017)

    - As per section 3.1 of Mozilla's Root Store Policy, we need a publishable (non-confidential) 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 their CA hierarchies, and that the CA does indeed follow these practices and meets the requirements of one or more of:
    - WebTrust "Principles and Criteria for Certification Authorities 2.0" or later and "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0" or later (as applicable to SSL certificate issuance) in WebTrust Program for Certification Authorities;
    - WebTrust "Principles and Criteria for Certification Authorities - Extended Validation SSL 1.4.5" or later in WebTrust Program for Certification Authorities;
    - "Requirements on CA practice", in ETSI TS 101 456 V1.4.3 or later version, Policy requirements for certification authorities issuing qualified certificates (only

applicable to electronic signature certificate issuance; applicable to either the "QCP public" or "QCP public + SSCD" certificate policies);

- "Requirements on CA practice", in ETSI TS 102 042 V2.3.1 or later version, Policy requirements for certification authorities issuing public key certificates (as applicable to the "EVCP" and "EVCP+" certificate policies, DVCP and OVCP certificate policies for publicly trusted certificates - baseline requirements, and any of the "NCP", "NCP+", or "LCP" certificate policies);
- "Trust Service Providers practice" in ETSI EN 319 411-1 v1.1.1 or later version Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, specifying a policy or policies appropriate to the trust bit(s) being applied for;
    - For Websites trust bit (need BR compliance audit) the CA must comply to EN 319 411-1 for "TLS" on level DV or OV or IV, and for "eMail" on level "LCP or NCP".
    - For EV treatment the CA must comply with EN 319 411-1 with the policy requirements identified for EVCP.
- "Trust Service Providers practice" in ETSI EN 319 411-2 v2.1.1 or later version Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, specifying a policy or policies appropriate to the trust bit(s) being applied for.
    - For QWACs the CA must comply with EN 319 411-2 with the policy requirements identified for QCP-w. Note: QCP-w defined in EN 319 411-2 builds on EVCP defined in EN 319 411-1.

- 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.

  Not applicable, we don't issue SSL Certificate.

    - Carefully review with your auditor:
        - https://www.mozilla.org//about/governance/policies/security-group/certs/policy/#required-audits
        - https://www.mozilla.org//about/governance/policies/security-group/certs/policy/#public-audit-information
- 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.
    - 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.
    - 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.
    - Government CAs
        - According to Mozilla's Root Store 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, ETSI EN 319 411, or WebTrust. The government's auditing agency should provide a statement about which of these their government criteria is equivalent to.

3. SSL Verification Procedures
    - If you are requesting to enable the Websites (SSL/TLS) trust bit...

      Not applicable, we are not requesting the 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
        - 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.
        - 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.

    - 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.

    - 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.

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.

        We use a rigorous verification process, describe in section 3.2 in CP.

        http://notarius.com/wp-content/uploads/2018/01/Notarius-PKI-Certificate-Policy.pdf

        - 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.

        - 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.

5. Code Signing Subscriber Verification Procedures

- No longer applicable: Mozilla is no longer accepting requests to enable the Code Signing trust bit, because we plan to remove the Code Signing trust bit in the next version of Mozilla's CA Certificate Policy.

  Not applicable.

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?
     - Specify the form factor that you use. Examples of multi-factor authentication include smartcards, client certificates, one-time-passwords, and hardware tokens.
     - 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.
     - If technical controls are used instead of multi-factor auth for any accounts, then specify what those technical controls are.

     As specify in the CP, all authorized positions in the PKI must use multi-factor. All sensible operation must be authorized by two people to complete operations.

     http://notarius.com/wp-content/uploads/2018/01/Notarius-PKI-Certificate-Policy.pdf, section 2.4, section 5.2.4, section 6.2.2, section 6.2.8

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.
     - Check for mis-issuance of certificates, especially for high-profile domains.

- Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness.
- Ensure Intrusion Detection System and other monitoring software is up-to-date.
- Confirm that you will be able to shut down certificate issuance quickly if you are alerted of intrusion.

We confirm that rigorous controls are applied. We are doing external scan on periodic period.

We are doing internal audit control each 3 months on all security account, network modification, and user computer control.

We are certified ISO27001 and ISO9001, that confirm that all best practices are used, documentation is kept up to date, and that they are vigorously followed. We are audited each year to comply with these certifications.