Information checklist for CAs applying for inclusion in Mozilla

In order to support cryptographic applications such as SSL/TLS connections to web and other servers, signed and encrypted email, and verification of digitally signed executable code objects, Firefox and other Mozilla-based products contain digital certificates and related metadata for multiple Certification Authorities (CAs). By including the CA certificates and various associated pre-set metadata values Mozilla-based products can recognize as valid the end entity certificates that are issued under the auspices of the CAs in question and are associated with, e.g., web servers, email senders, and software publishers.

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the [Mozilla CA certificate policy](http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy’s requirements have been satisfied. This information includes (but is not necessarily limited to) the following:

1. General information about the CA’s associated organization (i.e., the company, nonprofit organization, or government agency operating the CA), including
   1. Name. (This is the name by which the CA is most commonly known, e.g., "GeoTrust".)   
      E-GUVEN
   2. Website URL. (This should point to the English version of the web site if one exists.)

[www.e-guven.com](http://www.e-guven.com)

* 1. Organizational type. (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.)

E-Guven is a private corporation working in information security business for over 5 years and operating CA operation itself .E-Guven uses RSA’s KEON , CA platform for its CA operation and maintenance.

* 1. Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)

E-Guven serves certificates to mainly to Turkish market and in the next couple of years wants to expand their market to other countries. E-Guven certificates are used in Public projects as [www.turkiye.gov.tr](http://www.turkiye.gov.tr) and Mobile Signature as well.

E-Guven also develops B2B secure transaction projects.

1. For each root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified):
   1. The name of the root CA. (This is the so-called "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 name found within the Subject attribute of the root CA certificate itself.)

E-Guven

* 1. The root CA certificate. (Preferably this is in the form of a public URL through which the CA certificate can be directly downloaded. If no such public URL exists, a copy of the certificate should be obtained from the CA by other means and that copy should be attached to the bug report associated with the CA's request.)
  2. The X.509 certificate version. (For all but legacy roots this should be version 3.)   
     V3
  3. SHA-1 fingerprint. (The SHA-1 fingerprint of the root CA certificate.)

dd e1 d2 a9 01 80 2e 1d 87 5e 84 b3 80 7e 4b b1 fd 99 41 34

* 1. Type of signing key. (For example, RSA or ECC.)   
     RSA (2048 bits)
  2. Signing key parameters. (For RSA keys, the modulus length, for example, 1024 or 2048 bits. For ECC keys, the named curve, for example, NIST Curve P-256 or P-384. Note that although the Mozilla CA certificate policy does not specify a minimum modulus length, in practice a RSA modulus length of less than 2048 bits warrants further investigation. For example, is this a root created some time ago that is only now being proposed for inclusion? Was/is the root intended for use in low-end devices where performance was deemed an issue? Did the CA not think about the issue of modulus length at all? And so on. Similar considerations apply to ECC key sizes less than 256 bits.)   
     RSA (2048 bits)
  3. Valid from (YYYY-MM-DD). (The date from which the root CA certificate is valid.)   
     04.01.2007
  4. Valid to (YYYY-MM-DD). (The date until which the root CA certificate is valid.)

04.01.2017

* 1. A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate, including:
     1. A list (or summary description) of CAs with certificates signed by this root, including
        1. Any subordinate CAs 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.)
        2. Any subordinate CAs operated by third parties. (For example, this might include enterprise CAs for which this root CA has issued CA certificates. Note again 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 subordinates in question.)
           + If your root signs subordinate CAs that are operated by third parties, additional information may need to be provided as described in the [Subordinate CA Checklist.](https://wiki.mozilla.org/CA:SubordinateCA_checklist)
        3. Any other roots for which this root CA has issued cross-signing certificates. (If any such roots exist, it is important to note whether the roots in question are already included in the Mozilla root store or not.)   
           E-Guven root certificate has 3 intermediate CA . Their definitions are listed below.

E-Guven Mobile CA : Issues mobile certificates for end users.

E-Guven NES CA : Issues qualified electronic certificates for Turkish citizens.

E-Guven Secure Client Certificates : Used to issue Class3 certificates.

* + 1. A list of any other root CAs that have issued cross-signing certificates for this root CA. (Again, it is important to note whether any such roots are already included in the Mozilla root store or not.)
    2. The extent and nature of contractual and technical controls exercised over subordinate CAs, including
       1. Whether or not subordinate CAs are constrained to issue certificates only within certain domains. *[We need a technical description of how this is typically controlled.]*
       2. Whether or not subordinate CAs can create their own subordinates. *[We need a technical description of how this is typically controlled.]*
    3. The extent and nature of audits performed against subordinate CAs, including:   
       1. Whether or not subordinate CAs are included within the scope of any audit(s) done against the root CA.   
          All of our CA operation ( our CA and subordinate CA’s included) audited yearly for ISO:27001 criterias.
       2. Whether or not subordinate CAs are subject to third-party audits independent of any audit(s) done against the root CA.   
          These audits are done by Turkish Standarts Institute .
       3. The frequency at which any audit(s) for subordinate CAs are done.   
          Yearly
  1. Whether certificates are issued for any of the following purposes within the hierarchy rooted at this root CA certificate:
     1. Certificates usable for enabling web or other servers to support SSL/TLS connections. *[We need a description of the technical characteristics of such certificates.]*
     2. Certificates usable for signing and encrypting email messages (e.g., using S/MIME). *[We need a description of the technical characteristics of such certificates.]*   
        We issue Class3 certs for signing and encrypting email messages. They have relevant key usage fields.
     3. Certificates usable for digitally signing executable code objects. *[We need a description of the technical characteristics of such certificates.]*   
        We do not issue code signing certificates .
  2. If SSL certificates are issued within the hierarchy rooted at this root CA certificate:
     1. Whether or not the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. (Note that per the Mozilla policy this verification must be done *in addition to* any verification of the subscriber’s legal identity. Certificates for which *only* this level of verification is done are commonly referred to as DV certificates.)   
        This is a mandatory section for our SSL certs and also checked by our vettors from whois servers.
     2. Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber. (Certificates for which this level of verification is done are commonly referred to as OV certificates.)   
        We request a signed and stamped agreement from our subscribers declaring that they agree to our terms and conditions and their organization name.
     3. Whether verification of the certificate subscriber conforms to the Extended Validation Certificate Guidelines issued by the CAB Forum. (Certificates for which this level of verification is done are commonly referred to as EV certificates.)
  3. If email certificates are issued within the hierarchy rooted at this root CA certificate:
     1. Whether or not the email account associated with the email address in the certificate is verified to be owned/controlled by the certificate subscriber. (Note that per the Mozilla policy this verification must be done *in addition to* any verification of the subscriber’s legal identity.)   
        Email certificates are verified by E-Guven vettors manually by requesting a signed agreement and confirmation email.
     2. Whether or not the identity information in the certificate is verified to be that of the certificate subscriber.   
        It is verified . E-Guven verifies every information issued in certificates. For example if subscriber wants Organization name to be published in certificate he/she needs to prove it to us.
  4. If code signing certificates are issued within the hierarchy rooted at this root CA certificate, whether or not the identity information in the certificate is verified to be that of the certificate subscriber.
  5. If EV certificates are issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.
  6. Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. (There should be at least one example certificate for each of the major types of certificates issued, e.g., email vs. SSL vs. code signing, or EV vs. OV vs. DV. For SSL certificates this should also include URLs of one or more web servers using the certificate(s).)



* 1. Whether or not the validity of end entity and CA certificates issued within the hierarchy rooted at this root may be verified using Certificate Revocation Lists (CRLs) and, if so, the URL(s) at which the CRL(s) may be obtained.   
     <http://sil.e-guven.com/ElektronikBilgiGuvenligiASSSLClient/LatestCRL.crl>

<http://sil.e-guven.com/ElektronikBilgiGuvenligiASRoot/LatestCRL.crl>

<http://sil.e-guven.com/ElektronikBilgiGuvenligiASGKNESI/LatestCRL.crl>

* 1. Whether or not the validity of end entity and CA certificates issued within the hierarchy rooted at this root may be verified using the Online Certificate Status Protocol (OCSP) and, if so, the URL(s) for the associated OCSP responder(s).

<http://ocsp2.e-guven.com/ocsp.xuda>

* 1. The maximum time elapsing from the revocation of an end entity or CA certificate until CRLs and/or OCSP responders are updated to reflect that revocation.   
     8 hours for CRL  
     Online for OCSP
  2. 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. (These documents should be available at publicly accessible URLs, and should be in English or available in English translation.)
  3. 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.)