**Bugzilla ID:** 515425
**Bugzilla Summary:** Request to enable code-object-signing "trust bit" for DigiCert's three Root CAs

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, as per http://wiki.mozilla.org/CA:Information_checklist.

CA’s are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

| **General Information** | **Data** |
|---|---|
| CA Name | DigiCert |
| Website URL (English version) | http://www.digicert.com/ |
| Organizational type | Commercial |
| Primary market / customer base | DigiCert is a US-based commercial CA with headquarters in Lindon, UT. DigiCert provides digital certification and identity assurance services internationally to a variety of sectors including business, education, and government. |

**For Each Root CA** whose certificate is to be included in Mozilla (or whose metadata is to be modified)

| **Info Needed** | **Data** | **Data** | **Data** |
|---|---|---|---|
| Certificate Name | DigiCert Assured ID Root CA | DigiCert Global Root CA | DigiCert High Assurance EV Root CA |
| Cert summary | All three of these roots are already in NSS. They were approved for inclusion according to the Mozilla CA Policy in bug #364568. This request is to enable the Code Signing trust bit. | | |
| The root CA certificate URL | http://www.digicert.com/CACerts/DigiCertAssuredIDRootCA.crt | http://www.digicert.com/CACerts/DigiCertGlobalRootCA.crt | http://www.digicert.com/CACerts/DigiCertHighAssuranceEVRootCA.crt |
| SHA-1 fingerprint. | 05:63:B8:63:0D:62:D7:5A:BB:C8:AB:1E:4B:DF:B5:A8:99:B2:4D:43 | A8:98:5D:3A:65:E5:E5:C4:B2:D7:D6:6D:40:C6:DD:2F:B1:9C:54:36 | 5F:B7:EE:06:33:E2:59:DB:AD:OC:4C:9A:E6:D3:8F:1A:61:C7:DC:25 |
| Valid from | 2006-11-10 | 2006-11-10 | 2006-11-10 |
| Valid to | 2031-11-10 | 2031-11-10 | 2031-11-10 |
| Cert Version | 3 | 3 | 3 |
| Modulus length | 2048 | 2048 | 2048 |
| Test Website | https://catest.digicert-assured-id-ca-1.digicert.com/ | https://catest.digicert-global-ca-1.digicert.com/ | https://catest.digicert-high-assurance-ev-ca-1.digicert.com/ |
| CRL URL | http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl<br>http://crl3.digicert.com/DigiCertAssuredIDCA-1.crl<br>http://crl4.digicert.com/DigiCertAssuredIDCA-1.crl | http://crl3.digicert.com/DigiCertGlobalRootCA.crl<br>http://crl3.digicert.com/DigiCertGlobalCA-1.crl<br>http://crl4.digicert.com/DigiCertGlobalCA-1.crl | http://crl3.digicert.com/DigiCertHighAssuranceEVRootCA.crl<br>http://crl3.digicert.com/DigiCertHighAssuranceEVCA-1.crl<br>http://crl4.digicert.com/DigiCertHighAssuranceEVCA-1.crl |

| | | | |
|---|---|---|---|
| End-Entity CRL Update Frequency | CPS Section 2.3: CRLs for end-user Subscriber Certificates are issued at least once per day<br>End-Entity CRL Next Update: 7 days | | |
| OCSP Responder URL | http://ocsp.digicert.com/ | http://ocsp.digicert.com/ | http://ocsp.digicert.com/ |
| CA Hierarchy | Please provide a diagram and/or description of the CA hierarchy chaining up to each of these roots. | | |
| Sub CAs operated by 3rd parties | Are any of the sub-CAs for these roots operated by 3rd parties? If yes, please comment. If needed, please refer to https://wiki.mozilla.org/CA:SubordinateCA_checklist | | |
| cross-signing | Are any of these roots involved in cross-signing with other CAs? | | |
| Requested Trust Bits | Current: Websites (SSL/TLS), Email (S/MIME)<br>Requesting: Code Signing | | |
| If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV | OV, EV | OV, EV | OV, EV |
| EV policy OID(s) | Not EV-enabled in PSM | Not EV-enabled in PSM | 2.16.840.1.114412.2.1 |
| CP/CPS | All documents are in English.<br>Document Repository: http://www.digicert.com/ssl-cps-repository.htm<br>CPS: http://www.digicert.com/DigiCert_CPS.pdf<br>CPS for EV: http://www.digicert.com/DigiCert_EV-CPS.pdf | | |
| AUDIT | Audit Type: WebTrust CA<br>Auditor: KPMG<br>Auditor WebSite: http://kpmg.com/<br>Audit: http://www.digicert.com/regular-final-webtrust-report-2008.pdf (August 11, 2008) When is next one expected?<br>No issues noted in report.<br><br>Audit Type: WebTrust EV<br>Auditor: KPMG<br>Auditor WebSite: http://kpmg.com/<br>Audit: http://www.digicert.com/ev-final-webtrust-report.pdf (August 11, 2008) When is next one expected?<br>No issues noted in report.<br><br>When audit statements are provided by the company requesting CA inclusion/update 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.<br>Please recommend a contact and their email address at KPMG. | | |

**Review CPS sections dealing with subscriber verification** (section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify the domain referenced in an SSL cert is owned/controlled by the subscriber. In addition to verification of subscriber’s legal identity.
  - CPS Section 3.2.5: Authority to use domain name or IP address is confirmed by a WHOIS check or a practical demonstration of domain control to ensure that the Organization owns or controls the Domain Name or IP address.
    - The authority of the applicant's agent is confirmed with an authorized contact listed with the Domain Name Registrar ("Registrar") or through a person with administrative or technical control over the domain. The registered domain administrator or technical contact is asked to confirm the agent’s authorization to receive a Certificate for the URL requested. Contact information is obtained from WHOIS and reviewed by DigiCert validation personnel during the application process. After application submittal, authorization from the domain contact person and/or others such as persons with administrative control over the domain (e.g. webmaster@domain.com, administrator@domain.com, admin@domain.com, etc.) is received through one of the following methods:
      - These persons are contacted via a “Domain Control Validation” email and directed to a secure URL where at least one of them must enter their name and acknowledge that the person requesting the certificate has the right and authority to apply for the certificate to allow the application for a certificate to proceed. The name, email address and IP address of the organizational representative acknowledging authority are also recorded;
      - An Authorization Letter (e.g. Appendix A) is received from the Subscriber as explained in Sections 3.2.2, 4.1.1 and other portions of this CP/CPS;
      - A record of one of the foregoing is on file in the account for the Subscriber at DigiCert from a previous request for that domain (i.e. a Subscriber may pre-authorize its agent to perform all future renewals of the certificate); or
      - Other comparable methods of establishing authority are performed by DigiCert validation personnel.
    - CPS Section 4.2.1: DigiCert validation personnel review the application information provided by the Applicant to ensure
    - That the applicant has the right to use the domain name used in the application
      - Validated by reviewing domain name ownership records available publicly from the Domain Name Registrar
      - Validation may be supplemented in one of the following ways:
        - By communicating with the Administrative Contact listed in the WHOIS record
        - By communicating with generic emails which ordinarily are only available to persons with administrative control over the domain, for example, webmaster@domain.com, administrator@domain.com, admin@domain.com, etc.
        - By requiring a practical demonstration of domain control (e.g., requiring the Applicant to make a specified change to a live page on the given domain).
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber’s legal identity.
  - CPS Section 3.2.3: For Personal Email Certificates, DigiCert only verifies the applicant's email address control. An email is sent to the applicant at the email address to be included in the certificate. The applicant must respond affirmatively and acknowledge the

        certificate request at a specified DigiCert URL. The acknowledgement response establishes that the applicant has control over the email address. The name, email address and IP address of the individual providing the response are recorded.

    - CPS Section 3.2.5: Procedures similar to those above are also used to validate authority to receive an Enterprise Email Certificate. Authority and ability to use an email address are confirmed through email and an acknowledgement made at a secure URL. An email is sent to persons with administrative control over the domain, e.g. webmaster@domain.com, administrator@domain.com, admin@domain.com, etc., or as determined by the WHOIS record. The email requests that the person with administrative control over the domain visit a specified DigiCert URL where they enter their name and acknowledge that the person requesting the certificate has the right and authority to apply for the certificate. This confirms that the applicant has the right or permission to acquire a certificate under that domain. Similarly, another email is sent to the applicant at the email address to be included in the certificate and the applicant for the Enterprise Email Certificate must respond affirmatively and acknowledge the certificate request at a specified DigiCert URL, as described for Personal Email Certificates above in Section 3.2.3.

- Verify identity info in code signing certs is that of subscriber
    - CPS Section 3.2.2 details the elements used by DigiCert to authenticate the organization / subscriber identity.
    - CPS section 4.2.1: DigiCert validation personnel review the application information provided by the Applicant to ensure that the applicant is an accountable legal entity:
        - Documentation of organizational existence is obtained from available records, including those maintained by official government repositories and commercial providers of such information.
        - If necessary, information may be validated by requesting official company documentation, such as Business License, filed or certified Articles of Incorporation/Organization, Sales License or other relevant documents. For non-corporate applications, documentation listed in Section 3.2.3.

**Potentially Problematic Practices** (http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
    - SSL certs are OV
    - CPS: The validity period of a DigiCert-issued certificate is 1 year, 2 years or 3 years.
- Wildcard DV SSL certificates
    - SSL certs are OV
    - CPS: DigiCert issues server-specific, multi-server (unified communications), and wildcard (*.domain.com) SSL certificates.
- Delegation of Domain / Email validation to third parties
    - ?
- Issuing end entity certificates directly from roots
    - ?
- Allowing external entities to operate unconstrained subordinate CAs

  - ?
- Distributing generated private keys in PKCS#12 files
  - Not found.
- Certificates referencing hostnames or private IP addresses
  - CPS: DigiCert does issue Certificates for intranet use, and some certificates, including Unified Communications Certificates, may contain entries in the Subject Alternative Name extension that are not intended to be relied upon by the general public (e.g., they contain non-standard Top Level Domains like .local or they are addressed to an IP number space that has been allocated as private by RFC1918).
  - CPS: Authority to use domain name or IP address is confirmed by a WHOIS check or a practical demonstration of domain control to ensure that the Organization owns or controls the Domain Name or IP address.
- OCSP Responses signed by a certificate under a different root
  - Test websites work without error when OCSP is enforced.
- CRL with critical CIDP Extension
  - CRLs imported into Firefox without error.
- Generic names for CAs
  - Names are not generic.