Bugzilla ID: 908827
Bugzilla Summary: DigiCert Root Inclusion Request

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	DigiCert
Website URL	http://www.digicert.com/
Organizational type	Public corporation
Primark 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.
CA Contact Information	CA Email Alias: mteam@digicert.com CA Phone Number: 1-801-877-2100 Title / Department: Legal, Engineering or Operations

The request is to include 5 new root certs

These are DigiCert's next-generation certificates. With growing rumors of potential weakness in certain encryption and signing algorithms, DigiCert has decided to diversify the algorithms used in our new root certificates. This will ensure that we are able to meet the needs of our users in the coming years. We have both RSA and ECC versions of our new "Assured" and "Global" roots as we anticipate demand for both algorithms from each of these roots in the future.

- The new "Assured ID" roots will eventually replace the current DigiCert Assured ID Root CA certificate.
- The new "Global" roots will eventually replace the current DigiCert Global Root CA certificate.
- The new "Trusted" root will eventually replace the current DigiCert High Assurance EV Root CA certificate

The original DigiCert Root certificates should remain in the NSS root store until the new root certificates gain sufficient ubiquity to replace the originals, and the end entity certificates signed by the original roots all expire.

Technical information about the new Assured ID Root certificates

Certificate Name	DigiCert Assured ID Root G2	DigiCert Assured ID Root G3
Certificate Issuer Field	CN = DigiCert Assured ID Root G2 OU = www.digicert.com O = DigiCert Inc C = US	CN = DigiCert Assured ID Root G3 OU = www.digicert.com O = DigiCert Inc C = US
Certificate Summary	This SHA-256 root will eventually replace the SHA-1 "DigiCert Assured ID Root CA" certificate that was included in NSS via bug #364568. This root will have internally-operated intermediate certificates for issuing SSL, email, and code-signing certificates.	This is the ECC version of the SHA-1 "DigiCert Assured ID Root CA" certificate that was included in NSS via bug #364568. This root will have internally-operated intermediate certificates for issuing SSL, email, and code-signing certificates.

Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=794808	https://bugzilla.mozilla.org/attachment.cgi?id=794810
SHA1 Fingerprint	A1:4B:48:D9:43:EE:0A:0E:40:90:4F:3C:E0:A4:C0:91:93:51:5D:3F	F5:17:A2:4F:9A:48:C6:C9:F8:A2:00:26:9F:DC:0F:48:2C:AB:30:89
Valid From	2013-08-01	2013-08-01
Valid To	2038-01-15	2038-01-15
Cert Version	3	3
Cert Signature Algorithm	SHA-256	ECDSA Signature with SHA-384
Signing key parameters	2048-bit RSA	384-bit ECC
Test Website URL	https://assured-id-root-g2.digicert.com An error occurred during a connection to assured-id-root-g2.digicert.com. Invalid OCSP signing certificate in OCSP response. (Error code: sec_error_ocsp_invalid_signing_cert)	https://assured-id-root-g3.digicert.com
CRL URL	URL NextUpdate for CRLs of end-entity certs, both actual value and what's documented in CP/CPS.	http://crl3.digicert.com/DigiCertAssuredIDCAG3.crl http://crl4.digicert.com/DigiCertAssuredIDRootG3.crl
OCSP URL	OCSP URI in the AIA of end-entity certs Maximum expiration time of OCSP responses: ?	http://ocsp.digicert.com Maximum expiration time of OCSP responses: ?
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	DV, OV, and EV	DV, OV, and EV
EV Policy OID(s)	2.16.840.1.114412.2.1	2.16.840.1.114412.2.1
EV Test Results	Complete EV testing and attach success screenshot to bug. https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	Complete EV testing and attach success screenshot to bug. https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version

Technical information about the new Global Root certificates

Certificate Name	DigiCert Global Root G2	DigiCert Global Root G3
Certificate Issuer Field	CN = DigiCert Global Root G2 OU = www.digicert.com O = DigiCert Inc C = US	CN = DigiCert Global Root G3 OU = www.digicert.com O = DigiCert Inc C = US
Certificate Summary	This SHA-256 root will eventually replace the SHA-1 "DigiCert Global Root CA" certificate that was included in NSS via bug #364568. This root will have internally-operated intermediate certificates for issuing SSL, email, and code-signing certificates.	This is the ECC version of the SHA-1 "DigiCert Global Root CA" certificate that was included in NSS via bug #364568. This root will have internally-operated intermediate certificates for issuing SSL, email, and code-signing certificates.

Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=794811	https://bugzilla.mozilla.org/attachment.cgi?id=794812
SHA1 Fingerprint	DF:3C:24:F9:BF:D6:66:76:1B:26:80:73:FE:06:D1:CC:8D:4F:82:A4	7E:04:DE:89:6A:3E:66:6D:00:E6:87:D3:3F:FA:D9:3B:E8:3D:34:9E
Valid From	2013-08-01	2013-08-01
Valid To	2038-01-15	2038-01-15
Cert Version	3	3
Cert Signature Algorithm	SHA-256	ECDSA Signature with SHA-384
Signing key parameters	2048-bit RSA	384-bit ECC
Test Website URL	https://global-root-g2.digicert.com/ An error occurred during a connection to assured-id-root-g2.digicert.com. Invalid OCSP signing certificate in OCSP response. (Error code: sec_error_ocsp_invalid_signing_cert)	https://global-root-g3.digicert.com/
CRL URL	URL NextUpdate for CRLs of end-entity certs, both actual value and what's documented in CP/CPS.	http://crl3.digicert.com/DigiCertGlobalCAG3.crl http://crl4.digicert.com/DigiCertGlobalRootG3.crl
OCSP URL	OCSP URI in the AIA of end-entity certs Maximum expiration time of OCSP responses: ?	http://ocsp.digicert.com Maximum expiration time of OCSP responses: ?
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	DV, OV, and EV	DV, OV, and EV
EV Policy OID(s)	2.16.840.1.114412.2.1	2.16.840.1.114412.2.1
EV Test Results	Complete EV testing and attach success screenshot to bug. https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	Complete EV testing and attach success screenshot to bug. https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version

Technical information about the new Trusted Root certificate

Certificate Name	DigiCert Trusted Root G4
Certificate Issuer Field	CN = DigiCert Trusted Root G4 OU = www.digicert.com O = DigiCert Inc C = US
Certificate Summary	This SHA-384 root will eventually replace the SHA-1 "DigiCert High Assurance EV Root CA" cert that was included in NSS via bug #364568. This root will have internally-operated intermediate certs for issuing SSL, email, and code-signing certificates.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=794814

SHA1 Fingerprint	DD:FB:16:CD:49:31:C9:73:A2:03:7D:3F:C8:3A:4D:7D:77:5D:05:E4
Valid From	2013-08-01
Valid To	2038-01-15
Cert Version	3
Cert Signature Algorithm	SHA-384 with RSA
Signing key parameters	4096-bit RSA
Test Website	https://trusted-root-g4.digicert.com/
CRL URL	http://crl3.digicert.com/DigiCertTrustedServerCAG4.crl http://crl4.digicert.com/DigiCertTrustedRootG4.crl
OCSP URL	http://ocsp.digicert.com Maximum expiration time of OCSP responses: ?
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	DV, OV, and EV
EV Policy OID(s)	2.16.840.1.114412.2.1
EV Test Results	Complete EV testing and attach success screenshot to bug. https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version

CA Hierarchy information – Same info applies to all 5 root certs

CA Hierarchy	These root certificates will have internally-operated intermediate certificates for issuing SSL, email, and code-signing certificates.
Externally Operated SubCAs	None, and none planned.
Cross-Signing	None, and none planned.
Technical Constraints on Third-party Issuers	Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate

Verification Policies and Practices

Policy Documentation	All documents are in English. DigiCert Legal Repository: http://www.digicert.com/ssl-cps-repository.htm CP: http://www.digicert.com/docs/cps/DigiCert_CP_v405-May-2-2013.pdf CPS: http://www.digicert.com/docs/cps/DigiCert_CPS_v405-May-2-2013.pdf

Audits	Audit Type: WebTrust CA and WebTrust EV Auditor: KPMG Audit Report: https://cert.webtrust.org/SealFile?seal=1527&file=pdf (2013.07.12) EV Audit Report: https://cert.webtrust.org/SealFile?seal=1527&file=pdf (2013.07.12)
Baseline Requirements (SSL)	CP and CPS section 1.1: DigiCert conforms to the current version of the guidelines adopted by the Certification Authority/Browser Forum ("CAB Forum") when issuing publicly trusted certificates, including the Baseline Requirements for the Issuance and Management of Publicly‐Trusted Certificates ("Baseline Requirements") and the Guidelines for Extended Validation Certificates ("EV Guidelines") both of which are published at https://www.cabforum.org. If any inconsistency exists between this CPS and the Baseline Requirements or the EV Guidelines, then the EV Guidelines take precedence for EV Certificates and the Baseline Requirements take precedence for publicly trusted SSL certificates. Time‐stamping services are provided according to IETF RFC 3161 and other technical standards.
Organization Verification Procedures	CP and CPS section 3.2.2
SSL Verification Procedures	CP section 3.2.2: Domain names included in a publicly trusted SSL certificate must be verified in accordance with Section 11.1 of the Baseline Requirements. If a publicly‐trusted SSL certificate will contain an organization's name, then the Issuer CA (or an RA) shall verify the information about the organization and its legal existence in accordance with Section 11.2 of the Baseline Requirements using reliable third party and government databases or through other direct means of communication with the entity or jurisdiction governing the organization's legal creation, existence, or recognition. CPS section 3.2.2 -- DV SSL Server Certificates: DigiCert validates the Applicant's right to use or control the domain names that will be listed in the certificate using one or more of the following procedures: 1. Relying on publicly available records from the Domain Name Registrar, such as WHOIS or other DNS record information; 2. Communicating with one of the following email addresses: webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain, postmaster@domain, or any address listed in the technical, registrant, or administrative contact field of the domain's Registrar record; 3. 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); and/or 4. A domain authorization letter, provided the letter contains the signature of an authorized representative of the domain holder, a date that is on or after the certificate request, a list of the approved fully‐qualified domain name(s), and a statement granting the Applicant the right to use the domain names in the certificate. DigiCert also contacts the domain name holder using a reliable third‐party data source to confirm the authenticity of the domain authorization letter; and/or 5. A similar procedure that offers an equivalent level of assurance in the Applicant's ownership, control, or right to use the Domain Name. DigiCert verifies an included country code using (a) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address; (b) the ccTLD of the requested Domain Name; or (c) information provided by the Domain Name Registrar.

	CPS section 3.2.2 -- OV SSL Server Certificates: DigiCert validates the Applicant's right to use or control the Domain Name(s) that will be listed in the Certificate using the DV SSL Server Certificate validation procedures above. CPS section 3.2.2 – EV SSL Server Certificates: Information concerning organization identity related to the issuance of EV Certificates is validated in accordance with the EV Guidelines.
Email Address Verification Procedures	CPS section 3.2.2: DigiCert verifies organizational control over the email domain using authentication procedures similar to those used by DigiCert when establishing domain ownership by an organization before issuance of a DV or OV SSL Server Certificate. If the certificate contains organization information, DigiCert obtains documentation from the organization sufficient to confirm that the individual has an affiliation with the organization named in the certificate. For Authentication of Individual Identity for Client Certificates see CPS section 3.2.3 for details, because this depends on the verification level of the certificate. Level 1: Applicant's control of the email address or website listed in the certificate. For corporate email certificates, DigiCert verifies the organization and domain name listed in the certificate similar to an SSL Server Certificate. Level 2 verification includes in-person appearance before an RA. Level 3 is equivalent to NIST 800-63/Kantara Level 3 and FBCA CP Medium and Medium Hardware. Level 4 is for Biometric ID certs. CPS section 3.2.5: The authority of the individual requesting a certificate on behalf of an organization verified under section 3.2.2 is validated as follows: Level 1 Client Certificates – Personal (email certificates): Verifying that the individual has control over the email address listed in the certificate. Level 1 Client Certificates – Enterprise (email certificates): Having an individual with control over the domain visit a specified DigiCert URL where the person enters their name and acknowledges that the person requesting the certificate has the right and authority to apply for the certificate. In addition, an email is also sent to the Applicant at the email address that will be listed in the certificate. The Applicant for the Enterprise Email Certificate must respond and acknowledge the certificate request. Client Certificates Levels 2, 3 and 4 and PIV-I Certificates: Confirming with the organization that the individual is affiliated with the organization and that the individual has the authority to possess a certificate indicating the affiliation.
Code Signing Subscriber Verification Procedures	CPS and CP sections 3.2.2, 3.2.3, and section 3.2.5.
Multi-factor Authentication	Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes. See above.
CA Hierarchy	Yes. See above.
Audit Criteria	Yes. See above.
Document Handling of IDNs in CP/CPS	???
Revocation of Compromised Certificates	CPS and CP section 4.9
Verifying Domain Name Ownership	Yes. See above.
Verifying Email Address Control	Yes. See above.
Verifying Identity of Code Signing Certificate Subscriber	Yes. See above.
DNS names go in SAN	???
Domain owned by a Natural Person	???
OCSP	Yes. See above.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	CP section 6.3.2: OV SSL certs can be valid for 42 months. EV SSL certs can be valid for 27 months. What about DV SSL certs?
Wildcard DV SSL certificates	???
Email Address Prefixes for DV Certs	See above.
Delegation of Domain / Email validation to third parties	See above.
Issuing end entity certificates directly from roots	No. See above.
Allowing external entities to operate subordinate CAs	No. See above.
Distributing generated private keys in PKCS#12 files	???
Certificates referencing hostnames or private IP addresses	???
Issuing SSL Certificates for Internal Domains	???
OCSP Responses signed by a certificate under a different root	No
CRL with critical CIDP Extension	No
Generic names for CAs	No
Lack of Communication With End Users	No