Bugzilla ID: 617179
Bugzilla Summary: DigiCert 2048 Root and ECC Root Inclusion Request

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

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

Info Needed	Data	Data
Certificate Name	DigiCert Global Root CA	DigiCert High Assurance EV Root CA (ECC)
Cert summary / comments	This is the SHA256 version of the Global Root CA (SHA-1), which is already included in the NSS store per bug #364568.	This is the ECC version of DigiCert's High Assurance EV root CA certificate, which is already included in the NSS store per bug #364568.
Root Cert URL		
SHA-1 fingerprint	b6 7e 28 2c cb 89 0d 57 a6 91 96 9e 2c 33 f1 55 61 e0 89	d2 ab 41 9a 5c 14 48 9d 66 f8 03 b4 bc 66 27 9c 62 0a c0 0a
Valid from	2006-11-09	2010-0505
Valid to	2031-11-09	2037-05-05
Cert Version		
Signature Algorithm	sha256RSA	sha384ECDSA
Modulus length / key length or type of signing key (if ECC)		
Test Website	For testing purposes, please provide a URL to a website whose EV SSL cert chains up to this root.	For testing purposes, please provide a URL to a website whose EV SSL cert chains up to this root.

CRL URL	ARL and CRL URLs nextUpdate for CRLs of end-entity certs.	ARL and CRL URLs nextUpdate for CRLs of end-entity certs.
OCSP Responder URL	OCSP Responder URL Max time until OCSP responders updated to reflect end-entity revocation http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf 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."	OCSP Responder URL Max time until OCSP responders updated to reflect end-entity revocation http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf 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."
CA Hierarchy	Please describe and/or provide a diagram of the CA hierarchy for the SHA-1 version of the "DigiCert Global Root CA", and point out any planned changes for the hierarchy under this new root.	Please describe and/or provide a diagram of the CA hierarchy for the SHA-1 version of the "DigiCert High Assurance EV Root CA", and point out any planned changes for the hierarchy under this new root.
Externally operated subCAs	Does this root have any subordinate CAs that are operated by external third parties? If yes, please see https://wiki.mozilla.org/CA:SubordinateCA_checklist Are any of the sub-CAs that are operated by third-parties are or will be EV enabled? If the answer is yes, then please refer to http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf section 7.b.1 and section 37b.	Does this root have any subordinate CAs that are operated by external third parties? If yes, please see https://wiki.mozilla.org/CA:SubordinateCA_checklist Are any of the sub-CAs that are operated by third-parties are or will be EV enabled? If the answer is yes, then please refer to http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf section 7.b.1 and section 37b.
Cross-Signing	List any other root CAs that have issued cross-signing certificates for this root CA	List any other root CAs that have issued cross-signing certificates for this root CA
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	OV and EV	OV and EV
EV policy OID(s)	2.16.840.1.114412.2.1	2.16.840.1.114412.2.1
CP/CPS	All documents are in English. DigiCert Legal Repository: http://www.digicert.com/ssl-cps-repository.htm CP: http://www.digicert.com/http://www.digicert.com/DigiCert_CP_v401.pdf CPS: http://www.digicert.com/DigiCert_CPS_v401.pdf	

AUDIT	Audit Type: WebTrust CA Auditor: KPMG Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=1054 (2010.03.31) Audit Type: WebTrust EV Auditor: KPMG Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=1055 (2010.03.31)
Organization Identity Verification	CPS section 3.2.2, Authentication of Organization Identity: DigiCert verifies the organizational existence and identity of Applicants 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. If such efforts are insufficient to confirm the legal existence and identity of the subject, DigiCert requires the Applicant to submit official company documentation, such as a business license, filed or certified articles of incorporation/organization, tax certificate, corporate charter, official letter, sales license, or other relevant documents. DigiCert verifies the authority of the person requesting the certificate on behalf of an organization in accordance with Section 3.2.5. CPS section 3.2.3, Authentication of Individual Identity. For SSL Server Certs and Code Signing Certs… DigiCert shall verify an individual's entity using at least the following: 1. A legible copy of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). 2. Applicant's name and address are cross-checked for consistency with reliable data sources. 3. If further assurance is required, then DigiCert requires an additional form of identification, such as recent utility bills, financial account statements, credit card, college/university ID, or equivalent document type. 4. Confirming that the Applicant is able to receive communication by telephone, postal mail/courier, or fax. If DigiCert cannot verify the Applicant's identity using the procedures described above, then the Applicant must submit a Declaration of Identity that is witnessed and signed by a Registration Authority, Trusted Agent, notary, lawyer, accountant, postal carrier, or any entity certified by a State or National Government as authorized to confirm identities.
Domain Name Ownership / Control	Non-EV: CPS section 3.2.2: DigiCert also validates the Applicant's right to use the domain name that will be listed in the certificate. Domain name ownership is validated by: 1. Relying on publicly available records from the Domain Name Registrar; 2. Communicating with one of the following email addresses: webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain, postmaster@domain, and any address listed in the technical, registrant, or administrative contact field of the domain's Domain Name Registrar record; and/or 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). If a third-party makes the certificate application on behalf of the company listed in the Domain Name Registrar record, the

	third party must submit a document that shows the Applicant's right to use the domain name (such as the Domain Authorization Letter in Appendix A) that is signed by the Registrant (e.g. a domain owner's authorized representative) or the Administrative Contact on the Domain Name Registrar record. 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: Verifying the authority of the requester with an authorized contact listed with the Domain Name Registrar, through a person with control over the domain, or though an out-of-band confirmation with the organization. Communication to persons with control over the domain consists of emailing one or more of the following email addresses: webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain, postmaster@domain, or any address listed as a contact field of the domain's Domain Name Registrar record. EV: CPS section 3.2.2: EV Certificates are validated in accordance with the EV guidelines. CPS section 3.2.5: Verifying authority of the Contract Signer and Certificate Approver
Email Address Ownership / Control	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.
Identity of Code Signing Subscriber	For Code Signing Certificates… 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: Confirming the contact information and authority of the certificate requester with an authoritative source within the organization (e.g. corporate, legal, IT, HR, or other appropriate organizational sources) using a reliable means of communication; and Obtaining approval of the certificate request using a means of communication confirmed by the organization. CPS section 3.2.3, Authentication of Individual Identity. For SSL Server Certs and Code Signing Certs… DigiCert shall verify an individual's entity using at least the following: 1. A legible copy of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). 2. Applicant's name and address are cross-checked for consistency with reliable data sources. 3. If further assurance is required, then DigiCert requires an additional form of identification, such as recent utility bills, financial account statements, credit card, college/university ID, or equivalent document type. 4. Confirming that the Applicant is able to receive communication by telephone, postal mail/courier, or fax. If DigiCert cannot verify the Applicant's identity using the procedures described above, then the Applicant must submit a Declaration of Identity that is witnessed and signed by a Registration Authority, Trusted Agent, notary, lawyer, accountant, postal carrier, or any entity certified by a State or National Government as authorized to confirm identities.

Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information.
	• 1.1 Long-lived DV certificates
	  ○ SSL certs are OV.
	  ○ CPS section 3.3.1: SSL Server Certificates must go through re-verification at least every 6 years.
	• 1.2 Wildcard DV SSL certificates
	  ○ SSL certs are OV. DigiCert does allow for wildcard SSL certs that are OV.
	• 1.3 Email Address Prefixes for DV Certs
	  ○ DigiCert uses only the recommended list of email address prefixes.
	  ○ CPS section 3.2.5: Communication to persons with control over the domain consists of emailing one or more of the following email addresses: webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain, postmaster@domain, or any address listed as a contact field of the domain's Domain Name Registrar record.
	• 1.4 Delegation of Domain / Email validation to third parties
	  ○ ?
	• 1.5 Issuing end entity certificates directly from roots
	  ○ ?
	• 1.6 Allowing external entities to operate subordinate CAs

	○ ? • 1.7 Distributing generated private keys in PKCS#12 files ○ ? • 1.8 Certificates referencing hostnames or private IP addresses ○ ? • 1.9 Issuing SSL Certificates for Internal Domains ○ ? • 1.10 OCSP Responses signed by a certificate under a different root ○ ? • 1.11 CRL with critical CIDP Extension ○ ? • 1.12 Generic names for CAs ○ CN of the roots has DigiCert in them.