

Mozilla - CA Program

Case Information

Case Number	00000062	Case Record Type	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	DigiCert	Request Status	In Detailed CP/CPS Review

Additional Case Information

Subject	Enable EV for DigiCert roots	Case Reason
----------------	------------------------------	--------------------

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1165472
-----------------------------	---

General information about CA's associated organization

CA Email Alias 1	roots@digicert.com		
CA Email Alias 2			
Company Website	http://www.digicert.com/	Verified?	Verified
Organizational Type	Public Corporation	Verified?	Verified
Organizational Type (Others)		Verified?	Not Applicable
Geographic Focus	USA, Global	Verified?	Verified
Primary Market / Customer Base	Variety of sectors including business, education, and government.	Verified?	Verified
Impact to Mozilla Users	Enable EV treatment for previously included root certificates.	Verified?	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA/Required_or_Recommended_Practices	Recommended Practices Statement	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
------------------------------	---	--	--

CA's Response to Recommended Practices

1. Publicly Available CP and CPS: CPS section 2
 - 1.1 Revision Table, updated annually: CP/CPS section 1.2
 - 1.2 CAA Domains listed in CP/CPS: CPS section 4.2.1
[digicert.com](https://www.digicert.com), [digicert.ne.jp](https://www.digicert.ne.jp), [cybertrust.ne.jp](https://www.cybertrust.ne.jp), [symantec.com](https://www.symantec.com), [thawte.com](https://www.thawte.com), [geotrust.com](https://www.geotrust.com), [rapidssl.com](https://www.rapidssl.com), [digitalcertvalidation.com](https://www.digitalcertvalidation.com)
2. Audit Criteria: CP/CPS section 8
3. Revocation of Compromised Certificates: CP/CPS section 4.9
4. Verifying Domain Name Ownership: CPS section 3.2.2
5. Verifying Email Address Control: CP/CPS sections 3.2.2, 3.2.3
6. DNS names go in SAN: CP section 3.2.2, CPS section 4.2.1
7. OSCP: CP/CPS sections 4.9.9, 4.9.10
- OSCP SHALL NOT respond "Good" for unissued certs: tested
8. Network Security Controls: CP/CPS section 6.7

Verified? Verified

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices

https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices

Problematic Practices Statement

I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.

CA's Response to Problematic Practices

1. Long-lived Certificates: CP/CPS section 3.3.1
2. Non-Standard Email Address Prefixes for Domain Ownership Validation: CPS section 3.2.2
3. Issuing End Entity Certificates Directly From Roots: No
4. Distributing Generated Private Keys in PKCS#12 Files: CP/CPS section 6.1.2
https://bugzilla.mozilla.org/show_bug.cgi?id=1165472#c25
We never generate the private keys for SSL certs. We'll update our CPS to clarify this.
5. Certificates Referencing Local Names or Private IP Addresses: CP/CPS section 7.1.3
6. Issuing SSL Certificates for .int Domains: CP/CPS section 7.1.3
7. OSCP Responses Signed by a Certificate Under a Different Root: No. Tested.
8. Issuance of SHA-1 Certificates: CP/CPS section 7.1.3
9. Delegation of Domain / Email Validation to Third Parties: CPS section

Verified? Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	DigiCert Assured ID Root CA	Root Case No	R00000081
Request Status	In Detailed CP/CPS Review	Case Number	00000062

Certificate Data

Certificate Issuer Common Name	DigiCert Assured ID Root CA
O From Issuer Field	DigiCert Inc
OU From Issuer Field	www.digicert.com
Valid From	2006 Nov 10
Valid To	2031 Nov 10
Certificate Serial Number	0ce7e0e517d846fe8fe560fc1bf03039
Subject	CN=DigiCert Assured ID Root CA, OU= www.digicert.com , O=DigiCert Inc, C=US
Signature Hash Algorithm	sha1WithRSAEncryption
Public Key Algorithm	RSA 2048 bits
SHA-1 Fingerprint	05:63:B8:63:0D:62:D7:5A:BB:C8:AB:1E:4B:DF:B5:A8:99:B2:4D:43
SHA-256 Fingerprint	3E:90:99:B5:01:5E:8F:48:6C:00:BC:EA:9D:11:1E:E7:21:FA:BA:35:5A:89:BC:F1:DF:69:56:1E:3D:C6:32:5C
Subject + SPKI SHA256	
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This request is to enable EV treatment for the currently-included	Verified?	Verified
---------------------	---	-----------	----------

SHA-1 DigiCert Assured ID Root
CA certificate.

Root Certificate Download URL	https://www.digicert.com/CACerts/DigiCertAssuredIDRootCA.crt	Verified?	Verified
CRL URL(s)	http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl http://crl3.digicert.com/DigiCertAssuredIDTLSCA.crl	Verified?	Verified
OCSP URL(s)	http://ocsp.digicert.com	Verified?	Verified
Mozilla Trust Bits	Email; Websites	Verified?	Verified
SSL Validation Type	DV; OV; EV	Verified?	Verified
Mozilla EV Policy OID(s)	2.23.140.1.1	Verified?	Verified
Root Stores Included In	Microsoft; Mozilla	Verified?	Verified
Mozilla Applied Constraints	None	Verified?	Verified

Test Websites or Example Cert

Test Website - Valid	https://assured-id-root-ca.chain-demos.digicert.com/	Verified?	Verified
Test Website - Expired	https://assured-id-root-ca-expired.chain-demos.digicert.com/		
Test Website - Revoked	https://assured-id-root-ca-revoked.chain-demos.digicert.com/		
Example Cert			
Test Notes			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	https://certificate.revocationcheck.com/assured-id-root-ca.chain-demos.digicert.com No errors.	Verified?	Verified
CA/Browser Forum Lint Test	https://crt.sh/?caid=849&opt=cablint,zlint,x509lint&minNotBefore=2014-01-01 https://crt.sh/?caid=1911&opt=cablint,zlint,x509lint&minNotBefore=2018-01-01 Also ran for these CAids: 1687, 18099, 18106, 73277, 6511, 18100, 18152, 13644, 18118	Verified?	Verified

Test Website Lint Test	The lint testing shows errors, but I believe all of them have been addressed via m.d.s.policy and Bugzilla.	Verified?	Verified
EV Tested	ev-checker exited successfully: Success!	Verified?	Verified

CA Hierarchy Information

CA Hierarchy	This root has signed many subCAs, and they are disclosed in the CCADB and shown here: https://bug1165472.bmoattachments.org/attachment.cgi?id=8986325	Verified?	Verified
Externally Operated SubCAs	According to CPS sections 1.3 and 1.3.5, DigiCert's CAs have cross-certified with many organizations. See: https://bugzilla.mozilla.org/show_bug.cgi?id=1165472#c25 Our Sub CA policy prohibits all external Sub CAs for TLS certs with one exception - we'll sign a root for browsers requesting it.	Verified?	Verified
Cross Signing	See above, and CPS section 1.1, and CP section 2.1	Verified?	Verified
Technical Constraint on 3rd party Issuer	CPS section 1.3.2: Except for the authentication of domain control or IP address verification performed solely by DigiCert in accordance with Section 3.2.2, DigiCert may delegate the performance of certain functions to third party Registration Authorities (RA).	Verified?	Verified

Verification Policies and Practices

Policy Documentation	All documents are in English.	Verified?	Verified
CA Document Repository	http://www.digicert.com/ssl-cps-repository.htm	Verified?	Verified
CP Doc Language	English		
CP	https://www.digicert.com/wp-content/uploads/2018/01/DigiCert_CP_v414.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://www.digicert.com/wp-content/uploads/2018/01/DigiCert_CPS_v414.pdf	Verified?	Verified

Other Relevant Documents		Verified?	Not Applicable
Auditor	<u>Scott S. Perry CPA, PLLC</u>	Verified?	Verified
Auditor Location	<u>United States</u>	Verified?	Verified
Standard Audit	<u>https://cert.webtrust.org/SealFile?seal=2452&file=pdf</u>	Verified?	Verified
Standard Audit Type	WebTrust	Verified?	Verified
Standard Audit Statement Date	4/20/2018	Verified?	Verified
BR Audit	<u>https://cert.webtrust.org/SealFile?seal=2453&file=pdf</u>	Verified?	Verified
BR Audit Type	WebTrust	Verified?	Verified
BR Audit Statement Date	4/20/2018	Verified?	Verified
EV SSL Audit	<u>https://cert.webtrust.org/SealFile?seal=2454&file=pdf</u>	Verified?	Verified
EV SSL Audit Type	WebTrust	Verified?	Verified
EV SSL Audit Statement Date	4/20/2018	Verified?	Verified
BR Commitment to Comply	CPS sections 1.1, 2.1, 9.6.1 CP section 1.1, 2.1	Verified?	Verified
BR Self Assessment	<u>https://bugzilla.mozilla.org/attachment.cgi?id=8960346</u>	Verified?	Verified
SSL Verification Procedures	CP and CPS section 3.2.2	Verified?	Verified
EV SSL Verification Procedures	CP/CPS sections 3.2.2, 3.2.3, 3.2.5	Verified?	Verified
Organization Verification Procedures	CP/CPS sections 3.2.2, 3.2.3, 3.2.5	Verified?	Verified
Email Address Verification Procedures	CP/CPS sections 3.2.2, 3.2.3	Verified?	Verified
Code Signing Subscriber Verification Pro	N/A	Verified?	Not Applicable
Multi-Factor Authentication	CP/CPS section 5.2.	Verified?	Verified
Network Security	CP/CPS section 6.7	Verified?	Verified

Root Case Record # 2

Root Case Information

Root Certificate	DigiCert Global Root CA	Root Case No	R00000082
Request Status	In Detailed CP/CPS Review	Case Number	00000062
Certificate Data			
Certificate Issuer Common Name	DigiCert Global Root CA		
O From Issuer Field	DigiCert Inc		
OU From Issuer Field	www.digicert.com		
Valid From	2006 Nov 10		
Valid To	2031 Nov 10		
Certificate Serial Number	083be056904246b1a1756ac95991c74a		
Subject	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US		
Signature Hash Algorithm	sha1WithRSAEncryption		
Public Key Algorithm	RSA 2048 bits		
SHA-1 Fingerprint	A8:98:5D:3A:65:E5:E5:C4:B2:D7:D6:6D:40:C6:DD:2F:B1:9C:54:36		
SHA-256 Fingerprint	43:48:A0:E9:44:4C:78:CB:26:5E:05:8D:5E:89:44:B4:D8:4F:96:62:BD:26:DB:25:7F:89:34:A4:43:C7:01:61		
Subject + SPKI SHA256			
Certificate Version	3		
Technical Information about Root Certificate			
Certificate Summary	This request is to enable EV treatment for the currently-included SHA-1 DigiCert Global Root CA certificate.	Verified?	Verified
Root Certificate Download URL	https://www.digicert.com/CACerts/DigiCertGlobalRootCA.crt	Verified?	Verified
CRL URL(s)	http://crl3.digicert.com/DigiCertGlobalRootCA.crl http://crl3.digicert.com/ssca-sha2-g6.crl	Verified?	Verified

OCSP URL(s)	http://ocsp.digicert.com	Verified?	Verified
Mozilla Trust Bits	Email; Websites	Verified?	Verified
SSL Validation Type	DV; OV; EV	Verified?	Verified
Mozilla EV Policy OID(s)	2.23.140.1.1	Verified?	Verified
Root Stores Included In	Microsoft; Mozilla	Verified?	Verified
Mozilla Applied Constraints	None	Verified?	Verified

Test Websites or Example Cert

Test Website - Valid	https://global-root-ca.chain-demos.digicert.com/	Verified?	Verified
Test Website - Expired	https://global-root-ca-expired.chain-demos.digicert.com/		
Test Website - Revoked	https://global-root-ca-revoked.chain-demos.digicert.com/		
Example Cert			
Test Notes			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	https://certificate.revocationcheck.com/global-root-ca.chain-demos.digicert.com No errors.	Verified?	Verified
CA/Browser Forum Lint Test	https://crt.sh/?caid=980&opt=cablint,zlint,x509lint&minNotBefore=2014-01-01 https://crt.sh/?caid=81840&opt=cablint,zlint,x509lint&minNotBefore=2018-01-01	Verified?	Verified
Test Website Lint Test	Also tested for the following CA IDs: 81844, 65366, 65364, 37786, 26547, 1516, 981, 1191, 62127, 62148, 62133, 7327, 81845, 81842, 62143, 62131 The lint testing shows errors, but I believe all of them have been addressed via m.d.s.policy and Bugzilla.	Verified?	Verified
EV Tested	ev-checker exited successfully: Success!	Verified?	Verified

CA Hierarchy Information

CA Hierarchy	This root has many subCAs that are disclosed in the CCADB and shown here: https://bugzilla.mozilla.org/attachment.cgi?id=8986330	Verified?	Verified
Externally Operated SubCAs	According to CPS sections 1.3 and 1.3.5, DigiCert's CAs have cross-certified with many organizations. See: https://bugzilla.mozilla.org/show_bug.cgi?id=1165472#c25 Our Sub CA policy prohibits all external Sub CAs for TLS certs with one exception - we'll sign a root for browsers requesting it.	Verified?	Verified
Cross Signing	See above, and CPS section 1.1, and CP section 2.1	Verified?	Verified
Technical Constraint on 3rd party Issuer	CPS section 1.3.2: Except for the authentication of domain control or IP address verification performed solely by DigiCert in accordance with Section 3.2.2, DigiCert may delegate the performance of certain functions to third party Registration Authorities (RA).	Verified?	Verified

Verification Policies and Practices

Policy Documentation	All documents are in English.	Verified?	Verified
CA Document Repository	http://www.digicert.com/ssl-cps-repository.htm	Verified?	Verified
CP Doc Language	English		
CP	https://www.digicert.com/wp-content/uploads/2018/01/DigiCert_CP_v414.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://www.digicert.com/wp-content/uploads/2018/01/DigiCert_CPS_v414.pdf	Verified?	Verified
Other Relevant Documents		Verified?	Not Applicable
Auditor	Scott S. Perry CPA, PLLC	Verified?	Verified
Auditor Location	United States	Verified?	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=2452&file=pdf	Verified?	Verified

Standard Audit Type	WebTrust	Verified?	Verified
Standard Audit Statement Date	4/20/2018	Verified?	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=2453&file=pdf	Verified?	Verified
BR Audit Type	WebTrust	Verified?	Verified
BR Audit Statement Date	4/20/2018	Verified?	Verified
EV SSL Audit	https://cert.webtrust.org/SealFile?seal=2454&file=pdf	Verified?	Verified
EV SSL Audit Type	WebTrust	Verified?	Verified
EV SSL Audit Statement Date	4/20/2018	Verified?	Verified
BR Commitment to Comply	CPS sections 1.1, 2.1, 9.6.1 CP section 1.1, 2.1	Verified?	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8960346	Verified?	Verified
SSL Verification Procedures	CP and CPS section 3.2.2	Verified?	Verified
EV SSL Verification Procedures	CP/CPS sections 3.2.2, 3.2.3, 3.2.5	Verified?	Verified
Organization Verification Procedures	CP/CPS sections 3.2.2, 3.2.3, 3.2.5	Verified?	Verified
Email Address Verification Procedures	CP/CPS sections 3.2.2, 3.2.3	Verified?	Verified
Code Signing Subscriber Verification Pro	N/A	Verified?	Not Applicable
Multi-Factor Authentication	CP/CPS section 5.2	Verified?	Verified
Network Security	CP/CPS section 6.7	Verified?	Verified