# Mozilla - CA Program

## Case Information

| | | | |
|---|---|---|---|
| **Case Number** | 00000062 | **Case Record Type** | CA Owner/Root Inclusion Request |
| **CA Owner/Certificate Name** | DigiCert | **Request Status** | Need Information from CA |

## 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** | mteam@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** | United States and Global | **Verified?** | Verified |
| **Primary Market / Customer Base** | DigiCert provides digital certification and identity assurance services internationally to a variety of sectors including business, education, and government. | **Verified?** | Verified |
| **Impact to Mozilla Users** | Enable EV treatment for previously included root certificates. | **Verified?** | Verified |

## Response to Mozilla's list of Recommended Practices

| | | | |
|---|---|---|---|
| **Recommended Practices** | https://wiki.mozilla.org /CA:Recommended_Practices#CA_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** | NEED: Read and respond to https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices<br><br>Notes from previous request:<br>* IDN handling is referenced in Section 3.1.3 and 3.1.4 of the CPS. All IDNs are reviewed by validation staff to ensure they are not misleading or prone to confusion.<br>* Revocation of Compromised Certificates -- CPS and CP section 4.9<br>* All DNS names are listed in the SAN. Names in the CN field | **Verified?** | Need Response From CA |

are duplicated in the SAN.

### Response to Mozilla's list of Potentially Problematic Practices

| | | | |
|---|---|---|---|
| **Potentially Problematic Practices** | https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_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** | NEED: Read and respond to https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_practices<br><br>Notes from previous request:<br>* Long-lived SSL certificates CP section 6.3.2: OV SSL certs can be valid for 42 months. EV SSL certs can be valid for 27 months.<br>* DigiCert is currently issuing certificates with private/internal names. Per the BRs and Section 3.1.1 of our CPS, we plan to halt this process and revoke all existing certificates by the deadline. All such certificates currently being issued have an expiration date before October 1, 2016. DigiCert is also actively working with ICANN to ensure these names do not impact the release of the new gTLDs. | **Verified?** | Need Response From CA |

# Root Case Record # 1

### Root Case Information

| | | | |
|---|---|---|---|
| **Root Certificate Name** | DigiCert Assured ID Root CA | **Root Case No** | R00000081 |
| **Request Status** | Need Information from CA | **Case Number** | 00000062 |

### Additional Root Case Information

| | |
|---|---|
| **Subject** | Enable EV treatment for DigiCert Assured ID Root CA |

### Technical Information about Root Certificate

| | | | |
|---|---|---|---|
| **O From Issuer Field** | DigiCert Inc | **Verified?** | Verified |
| **OU From Issuer Field** | www.digicert.com | **Verified?** | Verified |
| **Certificate Summary** | This request is to enable EV treatment for the SHA-1 DigiCert Assured ID Root CA certificate which has 20 issuing CAs that issue certificates for servers. | **Verified?** | Verified |
| **Root Certificate Download URL** | https://www.digicert.com/CACerts /DigiCertAssuredIDRootCA.crt | **Verified?** | Verified |
| **Valid From** | 2006 Nov 10 | **Verified?** | Verified |
| **Valid To** | 2031 Nov 10 | **Verified?** | Verified |
| **Certificate Version** | 3 | **Verified?** | Verified |
| **Certificate Signature Algorithm** | SHA-1 | **Verified?** | Verified |
| **Signing Key Parameters** | 2048 | **Verified?** | Verified |

| | | | |
|---|---|---|---|
| **Test Website URL (SSL) or Example Cert** | NEED: Test website whose EV SSL cert chains up to this root. | **Verified?** | Need Response From CA |
| **CRL URL(s)** | http://crl3.digicert.com/DigiCertAssuredIDCA-1.crl<br>http://crl4.digicert.com/DigiCertAssuredIDCA-1.crl<br>http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl<br>http://crl4.digicert.com/DigiCertAssuredIDRootCA.crl<br>CRL issuing frequency for subordinate end-entity certificates: Daily | **Verified?** | Verified |
| **OCSP URL(s)** | http://ocsp.digicert.com<br>CPS section 4.10.1: OCSP information for subscriber certificates is updated at least every four days. | **Verified?** | Verified |
| **Revocation Tested** | NEED: put test website into http://certificate.revocationcheck.com/ and make sure there are no errors | **Verified?** | Need Response From CA |
| **Trust Bits** | Code; Email; Websites | **Verified?** | Verified |
| **SSL Validation Type** | DV; OV; EV | **Verified?** | Verified |
| **EV Policy OID(s)** | 2.16.840.1.114412.2.1 | **Verified?** | Verified |
| **EV Tested** | NEED: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version | **Verified?** | Need Response From CA |
| **Root Stores Included In** | Microsoft; Mozilla | **Verified?** | Verified |
| **Mozilla Applied Constraints** | None | **Verified?** | Verified |

## Digital Fingerprint Information

| | | | |
|---|---|---|---|
| **SHA-1 Fingerprint** | 05:63:B8:63:0D:62:D7:5A:BB:C8:AB:1E:4B:DF:B5:A8:99:B2:4D:43 | **Verified?** | Verified |
| **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 | **Verified?** | Verified |

## CA Hierarchy Information

| | | | |
|---|---|---|---|
| **CA Hierarchy** | 20 issuing CAs that issue certificates for servers<br>DigiCert Assured ID Root CA<br>\|----DigiCert Assured ID Code Signing CA-1<br>\|----DigiCert Grid Trust CA<br>\|----DigiCert Federated Trust CA<br>\|----DigicCert Assured ID Intermediate CA (SHA2)<br>\|----DigiCert Sha2 Assured ID CA<br>\|----DigiCert Sha2 Assured ID Code Signing CA<br>\|----DigiCert Document Signing CA<br>\|----DigiCert Grid Trust CA G2<br>\|----DigiCert Secure Auth CA<br>\|----TERENA Code Signing CA 3<br>\|----TERENA SSL CA 3<br>. . . (most if not all pathlengths of subordinate CAs = 0) | **Verified?** | Verified |
| **Externally Operated SubCAs** | NEED: Can externally-operated subCAs be created in this CA Hierarchy? | **Verified?** | Need Response From CA |

| | | | |
|---|---|---|---|
| **Cross Signing** | NEED: Has or will this root be involved in cross-signing with another root? | **Verified?** | Need Response From CA |
| **Technical Constraint on 3rd party Issuer** | NEED: Can a third party directly cause the issuance of an SSL certificate?<br>If yes, what constraints are in place? | **Verified?** | Need Response From CA |

## 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/docs/cps/DigiCert_CP_v408-1-Apr-2015-signed.pdf | **Verified?** | Verified |
| **CP Doc Language** | English | | |
| **CPS** | https://www.digicert.com/docs/cps/DigiCert_CPS_v408-1-Apr-2015-signed.pdf | **Verified?** | Verified |
| **Other Relevant Documents** | Subscriber Agreement: https://www.digicert.com/docs/agreements/DigiCert_SA.pdf<br>Warranty: https://www.digicert.com/docs/agreements/DigiCert_RPA.pdf | **Verified?** | Verified |
| **Auditor Name** | Scott S. Perry | **Verified?** | Verified |
| **Auditor Website** | https://www.scottperrycpa.com/ | **Verified?** | Verified |
| **Auditor Qualifications** | http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx | **Verified?** | Verified |
| **Standard Audit** | https://cert.webtrust.org/SealFile?seal=1867&file=pdf | **Verified?** | Verified |
| **Standard Audit Type** | WebTrust | **Verified?** | Verified |
| **Standard Audit Statement Date** | 4/24/2015 | **Verified?** | Verified |
| **BR Audit** | https://cert.webtrust.org/SealFile?seal=1868&file=pdf | **Verified?** | Verified |
| **BR Audit Type** | WebTrust | **Verified?** | Verified |
| **BR Audit Statement Date** | 4/24/2015 | **Verified?** | Verified |
| **EV Audit** | https://cert.webtrust.org/SealFile?seal=1869&file=pdf | **Verified?** | Verified |
| **EV Audit Type** | WebTrust | **Verified?** | Verified |
| **EV Audit Statement Date** | 4/24/2015 | **Verified?** | Verified |
| **BR Commitment to Comply** | CP and CPS section 1.1 | **Verified?** | Verified |
| **SSL Verification Procedures** | CPS section 3.2.2: 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:<br>1. Relying on publicly available records from the Domain Name Registrar, such as WHOIS or other DNS record information; | **Verified?** | Verified |

| | | | |
|---|---|---|---|
| | 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;<br>3. Requiring a practical demonstration of domain control (e.g., requiring the Applicant to make a specified change to a DNS zone file or a live page on the given domain); and/or<br>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;<br>and/or<br>5. A similar procedure that offers an equivalent level of assurance in the Applicant's ownership, control, or right to use the Domain Name. | | |
| **EV SSL Verification Procedures** | CPS section 3.2.2 – Information concerning organization identity related to the issuance of EV Certificates is validated in accordance with the EV Guidelines | **Verified?** | Verified |
| **Organization Verification Procedures** | CPS section 3.2.2: 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. DigiCert also verifies the identity and address of the Applicant using:<br>1. a reliable third party/government databases or through communication with the entity or jurisdiction governing the organization's legal creation, existence, or recognition;<br>2. a site visit;<br>3. an attestation letter that is signed by an accountant, lawyer, government official, or other reliable third party; or<br>4. for address only, a utility bill, bank statement, credit card statement, tax document, or other reliable form of identification.<br>DigiCert verifies any DBA included in a certificate using a third party or government source, attestation letter, or reliable form of identification. | **Verified?** | Verified |
| **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. | **Verified?** | Verified |

| | | | |
|---|---|---|---|
| | 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.<br><br>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.<br>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.<br>Level 2 verification includes in-person appearance before an RA.<br>Level 3 is equivalent to NIST 800-63/Kantara Level 3 and FBCA CP Medium and Medium Hardware.<br>Level 4 is for Biometric ID certs.<br><br>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: ... | | |
| **Code Signing Subscriber Verification Pro** | CPS and CP sections 3.2.2, 3.2.3, and section 3.2.5. | **Verified?** | Verified |
| **Multi-Factor Authentication** | NEED: Is multi-factor authentication required for all accounts that can directly cause the issuance of certificates in this CA Hierarchy? | **Verified?** | Need Response From CA |
| **Network Security** | CPS section 6.<br>We comply with the network security guidelines, have an intrusion detection system, and can turn off certificate issuance immediately in the event of a compromise. We undergo frequent pen tests by an independent third party to ensure that we are aware of any weaknesses in our system. Logs of sensitive systems are reviewed regularly, both manually and automatically, to detect anomalies and suspicious activity. | **Verified?** | Verified |

### Link to Publicly Disclosed and Audited subordinate CA Certificates

| | | | |
|---|---|---|---|
| **Publicly Disclosed & Audited subCAs** | https://www.digicert.com/digicert-root-certificates.htm | **Verified?** | Verified |

# Root Case Record # 2

### Root Case Information

| | | | |
|---|---|---|---|
| **Root Certificate Name** | DigiCert Global Root CA | **Root Case No** | R00000082 |
| **Request Status** | Need Information from CA | **Case Number** | 00000062 |

### Additional Root Case Information

| | |
|---|---|
| **Subject** | Enable EV treatment for DigiCert Global Root CA |

## Technical Information about Root Certificate

| | | | |
|---|---|---|---|
| **O From Issuer Field** | DigiCert Inc | **Verified?** | Verified |
| **OU From Issuer Field** | www.digicert.com | **Verified?** | Verified |
| **Certificate Summary** | This request is to enable EV treatment for the SHA-1 DigiCert Global Root CA certificate which has four internally-operated issuing CAs that issue certificates for clients and servers. | **Verified?** | Verified |
| **Root Certificate Download URL** | https://www.digicert.com/CACerts /DigiCertGlobalRootCA.crt | **Verified?** | Not Applicable |
| **Valid From** | 2006 Nov 10 | **Verified?** | Verified |
| **Valid To** | 2031 Nov 10 | **Verified?** | Verified |
| **Certificate Version** | 3 | **Verified?** | Verified |
| **Certificate Signature Algorithm** | SHA-1 | **Verified?** | Verified |
| **Signing Key Parameters** | 2048 | **Verified?** | Verified |
| **Test Website URL (SSL) or Example Cert** | NEED: Test website whose EV SSL cert chains up to this root. | **Verified?** | Need Response From CA |
| **CRL URL(s)** | http://crl3.digicert.com /DigiCertGlobalRootCA.crl http://crl4.digicert.com /DigiCertGlobalRootCA.crl http://crl3.digicert.com/ssca-sha2-g1.crl http://crl4.digicert.com/ssca-sha2-g1.crl CRL issuing frequency for subordinate end-entity certificates: Daily | **Verified?** | Verified |
| **OCSP URL(s)** | http://ocsp.digicert.com CPS section 4.10.1: OCSP information for subscriber certificates is updated at least every four days. | **Verified?** | Verified |
| **Revocation Tested** | NEED: put test website into http://certificate.revocationcheck.com/ and make sure there are no errors | **Verified?** | Need Response From CA |
| **Trust Bits** | Code; Email; Websites | **Verified?** | Verified |
| **SSL Validation Type** | DV; OV; EV | **Verified?** | Verified |
| **EV Policy OID(s)** | 2.16.840.1.114412.2.1 | **Verified?** | Verified |
| **EV Tested** | NEED: https://wiki.mozilla.org /PSM:EV_Testing_Easy_Version | **Verified?** | Need Response From CA |
| **Root Stores Included In** | Microsoft; Mozilla | **Verified?** | Verified |
| **Mozilla Applied Constraints** | None | **Verified?** | Verified |

## Digital Fingerprint Information

| | | | |
|---|---|---|---|
| **SHA-1 Fingerprint** | A8:98:5D:3A:65:E5:E5:C4:B2:D7:D6:6D:40:C6:DD:2F:B1:9C:54:36 | **Verified?** | Verified |
| **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 | **Verified?** | Verified |

## CA Hierarchy Information

| | | | |
|---|---|---|---|
| **CA Hierarchy** | Four issuing CAs that issue certificates for clients and servers<br>DigiCert Global Root CA<br>\|----DigiCert ECC Secure Server CA<br>\|----DigiCert SHA2 Secure Server CA<br>\|----DigiCert Secure Server CA<br>\|----DigiCert Global CA-1<br>. . . (most if not all pathlengths of subordinate CAs = 0) | **Verified?** | Verified |
| **Externally Operated SubCAs** | NEED: Can externally-operated subCAs be created in this CA Hierarchy? | **Verified?** | Need Response From CA |
| **Cross Signing** | NEED: Has or will this root be involved in cross-signing with another root? | **Verified?** | Need Response From CA |
| **Technical Constraint on 3rd party Issuer** | NEED: Can a third party directly cause the issuance of an SSL certificate?<br>If yes, what constraints are in place? | **Verified?** | Need Response From CA |

## 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/docs/cps/DigiCert_CP_v408-1-Apr-2015-signed.pdf | **Verified?** | Verified |
| **CP Doc Language** | English | | |
| **CPS** | https://www.digicert.com/docs/cps/DigiCert_CPS_v408-1-Apr-2015-signed.pdf | **Verified?** | Verified |
| **Other Relevant Documents** | Subscriber Agreement: https://www.digicert.com/docs/agreements/DigiCert_SA.pdf<br>Warranty: https://www.digicert.com/docs/agreements/DigiCert_RPA.pdf | **Verified?** | Verified |
| **Auditor Name** | Scott S. Perry | **Verified?** | Verified |
| **Auditor Website** | https://www.scottperrycpa.com/ | **Verified?** | Verified |
| **Auditor Qualifications** | http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx | **Verified?** | Verified |
| **Standard Audit** | https://cert.webtrust.org/SealFile?seal=1867&file=pdf | **Verified?** | Verified |
| **Standard Audit Type** | WebTrust | **Verified?** | Verified |
| **Standard Audit Statement Date** | 4/24/2015 | **Verified?** | Verified |

| | | | |
|---|---|---|---|
| **BR Audit** | https://cert.webtrust.org/SealFile?seal=1868&file=pdf | **Verified?** | Verified |
| **BR Audit Type** | WebTrust | **Verified?** | Verified |
| **BR Audit Statement Date** | 4/24/2015 | **Verified?** | Verified |
| **EV Audit** | https://cert.webtrust.org/SealFile?seal=1869&file=pdf | **Verified?** | Verified |
| **EV Audit Type** | WebTrust | **Verified?** | Verified |
| **EV Audit Statement Date** | 4/24/2015 | **Verified?** | Verified |
| **BR Commitment to Comply** | CP and CPS section 1.1 | **Verified?** | Verified |
| **SSL Verification Procedures** | CPS section 3.2.2: 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:<br>1. Relying on publicly available records from the Domain Name Registrar, such as WHOIS or other DNS record information;<br>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;<br>3. Requiring a practical demonstration of domain control (e.g., requiring the Applicant to make a specified change to a DNS zone file or a live page on the given domain); and/or<br>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<br>5. A similar procedure that offers an equivalent level of assurance in the Applicant's ownership, control, or right to use the Domain Name. | **Verified?** | Verified |
| **EV SSL Verification Procedures** | CPS section 3.2.2 – Information concerning organization identity related to the issuance of EV Certificates is validated in accordance with the EV Guidelines. | **Verified?** | Verified |
| **Organization Verification Procedures** | CPS section 3.2.2: 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. DigiCert also verifies the identity and address of the Applicant using: | **Verified?** | Verified |

| | | | |
|---|---|---|---|
| | 1. a reliable third party/government databases or through communication with the entity or jurisdiction governing the organization's legal creation, existence, or recognition;<br>2. a site visit;<br>3. an attestation letter that is signed by an accountant, lawyer, government official, or other reliable third party; or<br>4. for address only, a utility bill, bank statement, credit card statement, tax document, or other reliable form of identification.<br>DigiCert verifies any DBA included in a certificate using a third party or government source, attestation letter, or reliable form of identification. | | |
| **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.<br>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.<br><br>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.<br>Level 1: Applicant's control of the email address or website listed in the certificate.<br>For corporate email certificates, DigiCert verifies the organization and domain name listed in the certificate similar to an SSL Server Certificate.<br>Level 2 verification includes in-person appearance before an RA.<br>Level 3 is equivalent to NIST 800-63/Kantara Level 3 and FBCA CP Medium and Medium Hardware.<br>Level 4 is for Biometric ID certs.<br><br>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: ... | **Verified?** | Verified |
| **Code Signing Subscriber Verification Pro** | CPS and CP sections 3.2.2, 3.2.3, and section 3.2.5. | **Verified?** | Verified |
| **Multi-Factor Authentication** | Multi-factor authentication is required on all accounts that can cause issuance. All such accounts are internal DigiCert internal accounts. | **Verified?** | Verified |
| **Network Security** | CPS section 6.<br>We comply with the network security guidelines, have an intrusion detection system, and can turn off certificate issuance immediately in the event of a compromise. We undergo frequent pen tests by an independent third party to ensure that we are aware of any weaknesses in our system. Logs of | **Verified?** | Verified |

| | |
|---|---|
| | sensitive systems are reviewed regularly, both manually and automatically, to detect anomalies and suspicious activity. |

## Link to Publicly Disclosed and Audited subordinate CA Certificates

| | | | |
|---|---|---|---|
| **Publicly Disclosed & Audited subCAs** | https://www.digicert.com/digicert-root-certificates.htm | **Verified?** | Verified |