## Public Root: DigiCert Assured ID Root CA

| Field | Criticality Flag | Value | Comments |
|---|---|---|---|
| Certificate | | | |
| tbsCertificate | | | Fields to be signed. |
| **version** | | 2 | Integer Value of "2" for Version 3 certificate. |
| **serialNumber** | | 5e ca d5 00 e5 1e d3 b5 bc 8e 23 e6 21 f8 91 9f | |
| **signature** | | | |
| AlgorithmIdentifier | | | Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA. |
| algorithm | | 1.2.840.113549.1.1.5 | sha1withRSAEncryption |
| parameters | | NULL | |
| **issuer** | | | |
| RelativeDistinguishedName | | | Matches Subject DN. |
| countryName (2.5.4.6) | | US | |
| organizationName (2.5.4.10) | | DigiCert Inc | |
| organizationalUnitName (2.5.4.11) | | www.digicert.com | |
| commonName (2.5.4.3) | | DigiCert Assured ID Root CA | |
| **validity** | | | |
| notBefore Time | | 2006/11/09 5:00:00 PM | utcTime - YYMMDDHHMMSSZ |
| notAfter Time | | 2031/11/09 05:00:00 PM | utcTime - YYMMDDHHMMSSZ |
| **subject** | | | |
| RelativeDistinguishedName | | | Matches Issuer DN. |
| countryName (2.5.4.6) | | US | |
| organizationName (2.5.4.10) | | DigiCert Inc | |
| organizationalUnitName (2.5.4.11) | | www.digicert.com | |
| commonName (2.5.4.3) | | DigiCert Assured ID Root CA | |
| **subjectPublicKeyInfo** | | | |
| algorithm | | | |
| AlgorithmIdentifier | | | Public key algorithm associated with the public key. |
| algorithm | | 1.2.840.113549.1.1.1 | RSA Encryption |
| parameters | | NULL | |
| subjectPublicKey | | AD 0E 15 CE E4 43 80 5C B1 87 … (2048-bit Public Key) | |
| | | 65537 | |
| **required extensions** | | | |
| **keyUsage (2.5.29.15)** | **TRUE** | 86 | |
| digitalSignature | | 1 | |
| nonRepudiation | | 0 | |
| keyEncipherment | | 0 | |
| dataEncipherment | | 0 | |
| keyAgreement | | 0 | |
| keyCertSign | | 1 | |
| cRLSign | | 1 | |
| encipherOnly | | 0 | |
| decipherOnly | | 0 | |
| **basicConstraints (2.5.29.19)** | **TRUE** | | |
| cA | | Y | |
| pathLenConstraint | | None | |
| **subjectKeyIdentifier (2.5.29.14)** | | 45 eb a2 af f4 92 cb 82 31 2d 51 8b a7 a7 21 9d f3 6d c8 0f | |
| **authorityKeyIdentifier (2.5.29.35)** | | 45 eb a2 af f4 92 cb 82 31 2d 51 8b a7 a7 21 9d f3 6d c8 0f | |
| **Signature** | | | |
| signatureAlgorithm | | 1.2.840.113549.1.1.5 | sha1withRSAEncryption |
| **signature** | | 77 EC 70 CE 1A EF 87 26 42 86 4B ED 14 8E A3 … | |

**NOTE: for IGTF Trust**

## Public Trust subCA: DigiCert Grid Trust CA

| Field | Criticality Flag | Value | Comments |
|---|---|---|---|
| Certificate | | | |
| tbsCertificate | | | Fields to be signed. |
| **version** | | 2 | Integer Value of "2" for Version 3 certificate. |
| **serialNumber** | | 07 15 56 1f e5 7f 30 be 17 89 89 23 c3 3a 44 50 | |
| **signature** | | | |
| AlgorithmIdentifier | | | Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA. |
| algorithm | | 1.2.840.113549.1.1.5 or 1.2.840.113549.1.1.11 | sha1withRSAEncryption or Sha256WithRSAEncryption |
| parameters | | NULL | |
| **issuer** | | | |
| RelativeDistinguishedName | | | |
| countryName (2.5.4.6) | | US | |
| organizationName (2.5.4.10) | | DigiCert Inc | |
| organizationalUnitName (2.5.4.11) | | www.digicert.com | |
| commonName (2.5.4.3) | | DigiCert Assured ID Root CA | |
| **validity** | | | |
| notBefore Time | | Wednesday, December 07, 2011 5:00:00 AM | utcTime - YYMMDDHHMMSSZ |
| notAfter Time | | Monday, December 07, 2026 5:00:00 AM | utcTime - YYMMDDHHMMSSZ |
| **subject** | | | |
| RelativeDistinguishedName | | | |
| countryName (2.5.4.6) | | US | |
| organizationName (2.5.4.10) | | DigiCert Grid | |
| organizationalUnitName (2.5.4.11) | | www.digicert.com | |
| commonName (2.5.4.3) | | DigiCert Grid Trust CA | |
| **subjectPublicKeyInfo** | | | |
| algorithm | | | |
| AlgorithmIdentifier | | | Public key algorithm associated with the public key. |
| algorithm | | 1.2.840.113549.1.1.1 | RSA Encryption |
| parameters | | NULL | |
| subjectPublicKey | | … (2048-bit Public Key) | |
| | | 65537 | |
| **required extensions** | | | |
| **keyUsage (2.5.29.15)** | **TRUE** | 86 | |
| digitalSignature | | 1 | To faciliate direct OCSP signing if required |
| nonRepudiation | | 0 | |
| keyEncipherment | | 0 | |
| dataEncipherment | | 0 | |
| keyAgreement | | 0 | |
| keyCertSign | | 1 | |
| cRLSign | | 1 | |
| encipherOnly | | 0 | |
| decipherOnly | | 0 | |
| **basicConstraints (2.5.29.19)** | **TRUE** | | |
| cA | | Y | |
| pathLenConstraint | | 0 | |
| **authorityInfoAccess (1.3.6.1.5.5.7.1.1)** | FALSE | | authorityInfoAccess consists of a sequence of accessMethod |
| accessMethod | | On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) | |
| accessLocation | | http://ocsp.digicert.com | GeneralName (uniformResourceIdentifier) |
| accessMethod | | id-ad-caIssuers (1.3.6.1.5.5.7.48.2) | When this access method is used, the access location should |
| accessLocation | | http://cacerts.digicert.com/DigiCertAssuredIDRootCA.p7c | GeneralName (uniformResourceIdentifier) |
| **cRLDistributionPoints (2.5.29.31)** | FALSE | | This extension is required in all CA certificates and must |
| DistributionPointName | | | |
| fullName | | http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl | |
| DistributionPointName | | | |
| fullName | | http://crl4.digicert.com/DigiCertAssuredIDRootCA.crl | |
| **extendedKeyUsage (2.5.29.37)** | FALSE | Not Present | |
| **certificatePolicies (2.5.29.32)** | FALSE | | |
| policyIdentifier | | 2.16.840.1.114412.0.2.4 | |
| policyQualifierID | | http://www.digicert.com/ssl-cps-repository.htm | Type = CPS |
| policyQualifierInfo | | Any use of this Certificate constitutes acceptance of the DigiCert CP/CPS and the Relying Party Agreement which limit liability and are incorporated herein by reference. | Type = User Notice |

| | | | |
|---|---|---|---|
| **subjectKeyIdentifier (2.5.29.14)** | FALSE | 61 97 a4 9b 29 98 01 9b 5a ff 87 e6 74 ef 30 83 cc 68 b4 c8 | |
| **authorityKeyIdentifier (2.5.29.35)** | FALSE | 45 eb a2 af f4 92 cb 82 31 2d 51 8b a7 a7 21 9d f3 6d c8 0f | |
| **Signature** | | | |
| signatureAlgorithm | | 1.2.840.113549.1.1.5 or 1.2.840.113549.1.1.11 | sha1withRSAEncryption or Sha256WithRSAEncryption |
| **signature** | | | |

**NOTE: GFD125 compliant, for IGTF Accreditation**

**Grid Host : Grid Service or Host Certificate - Public Trust**

| Field | Criticality Flag | Value | Comments |
|---|---|---|---|
| Certificate | | | |
| tbsCertificate | | | Fields to be signed. |
| **version** | | 2 | Integer Value of "2" for Version 3 certificate. |
| **serialNumber** | | INTEGER | Unique positive integer. |
| **signature** | | | |
| AlgorithmIdentifier | | | Must match Algorithm Identifier in signatureAlgorithm field. The |
| algorithm | | 1.2.840.113549.1.1.5 or 1.2.840.113549.1.1.11 | sha1withRSAEncryption or Sha256WithRSAEncryption |
| parameters | | NULL | |
| **issuer** | | | |
| RelativeDistinguishedName | | | |
| countryName (2.5.4.6) | | US | |
| organizationName (2.5.4.10) | | DigiCert Grid | |
| organizationalUnitName (2.5.4.11) | | www.digicert.com | |
| commonName (2.5.4.3) | | DigiCert Grid Trust CA | |
| **validity** | | | |
| notBefore | | (issue date) | |
| utcTime | | YYMMDDHHMMSSZ | Use for dates up to and including 2049. |
| generalTime | | YYYYMMDDHHMMSSZ | Use for dates after 2049 |
| notAfter | | (issue date + up to 13 months) | |
| utcTime | | YYMMDDHHMMSSZ | Use for dates up to and including 2049. |
| generalTime | | YYYYMMDDHHMMSSZ | Use for dates after 2049 |
| **subject** | | | |
| RelativeDistinguishedName | | | |
| countryName (2.5.4.6) | | US | Required when multiple DC are NOT used |
| domainComponent (0.9.2342.19200300.100.1.25) | | com | If not multiple DC, then single Country is permitted i.e.C=US |
| domainComponent (0.9.2342.19200300.100.1.25) | | DigiCert-Grid or DigiCertGrid | If not multiple DC, then single Country is permitted i.e.C=US |
| organizationName (2.5.4.10) | | If C=US, then O=DigiCert Grid, else optional | Optional except where Country is used, then compulsory to at least use use "O=DigiCert Grid" |
| organizationalUnitName (2.5.4.11) | | Services | OU= Services |
| commonName (2.5.4.3) | | (FQDN) | FQDN may be prefixed with service type identifier e.g. host/FQDN |
| **subjectPublicKeyInfo** | | | |
| algorithm | | | |
| AlgorithmIdentifier | | | Public key algorithm associated with the public key. |
| algorithm | | 1.2.840.113549.1.1.1 | RSA Encryption |
| RSAParameters | | NULL | For RSA, parameters field is populated with NULL. |
| subjectPublicKey | | BIT STRING | Modulus of at least 2048 bits. |
| **required extensions** | | | |
| **authorityKeyIdentifier** | FALSE | OCTET STRING | Derived using the SHA-1 hash of the public key. |
| **subjectKeyIdentifier** | FALSE | OCTET STRING | Derived using the SHA-1 hash of the public key. |
| **keyUsage** | TRUE | | |
| digitalSignature | | 1 | must be asserted. |
| nonRepudiation | | 0 | communications devices. |
| keyEncipherment | | 1 | Must be asserted |
| dataEncipherment | | 1 | May be asserted |
| keyAgreement | | 0 | |
| keyCertSign | | 0 | |
| cRLSign | | 0 | |
| encipherOnly | | 0 | |
| decipherOnly | | 0 | |
| **basicConstraints (2.5.29.19)** | **TRUE** | | |
| End Entity | | Y | |
| pathLenConstraint | | None | |
| **certificatePolicies** | FALSE | | |
| PolicyInformation | | | |
| policyIdentifier | | 1.2.840.113612.5.2.2.1 | IGTF Classic OID |
| policyIdentifier | | 2.16.840.1.114412.1.31.1 | DigiCert Grid Classic Host Public Trust |
| policyIdentifier | | 1.2.840.113612.5.2.3.3.2 | IGTF 1SCP Host |
| **cRLDistributionPoints (2.5.29.31)** | FALSE | | |
| DistributionPointName | | | |
| fullName | | http://crl3.digicert.com/DigiCertGridTrustCA.crl | |

| | | | |
|---|---|---|---|
| DistributionPointName | | | |
| fullName | | http://crl4.digicert.com/DigiCertGridTrustCA.crl | |
| **authorityInfoAccess (1.3.6.1.5.5.7.1.1)** | FALSE | | |
| accessMethod | | On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) | |
| accessLocation | | http://ocsp.digicert.com | GeneralName (uniformResourceIdentifier) |
| accessMethod | | id-ad-calssuers (1.3.6.1.5.5.7.48.2) | |
| accessLocation | | http://cacerts.digicert.com/DigiCertGridTrustCA.crt | GeneralName (uniformResourceIdentifier) |
| **extKeyUsage** | FALSE | | |
| keyPurposeID | | serverAuth ( 1.3.6.1.5.5.7.3.1) | |
| | | clientAuth ( 1.3.6.1.5.5.7.3.2) | Optional |
| **subjectAltName** | FALSE | | |
| dNSName | | IA5String | This field contains the DNS name of the subject |
| rfc822Name | | Optional (IA5String) | Electronic mail address of the service/host administration (Optional) |
| **Signature** | | | |
| signatureAlgorithm | | 1.2.840.113549.1.1.5 or 1.2.840.113549.1.1.11 | sha1withRSAEncryption or Sha256WithRSAEncryption |
| **signature** | | | |

**NOTE: GFD125 compliant, for IGTF Accreditation**

## Grid Client : Dual Purpose Grid Certificate Profile - Public Trust

| Field | Criticality Flag | Value | Comments |
|---|---|---|---|
| Certificate | | | |
| tbsCertificate | | | Fields to be signed. |
| **version** | | 2 | Integer Value of "2" for Version 3 certificate. |
| **serialNumber** | | INTEGER | Unique positive integer. |
| **signature** | | | |
| AlgorithmIdentifier | | | Must match Algorithm Identifier in signatureAlgorithm field. The |
| algorithm | | 1.2.840.113549.1.1.5 or 1.2.840.113549.1.1.11 | sha1withRSAEncryption or Sha256WithRSAEncryption |
| parameters | | NULL | |
| **issuer** | | | |
| RelativeDistinguishedName | | | |
| countryName (2.5.4.6) | | US | |
| organizationName (2.5.4.10) | | DigiCert Grid | |
| organizationalUnitName (2.5.4.11) | | www.digicert.com | |
| commonName (2.5.4.3) | | DigiCert Grid Trust CA | |
| **validity** | | | |
| notBefore | | (issue date) | |
| utcTime | | YYMMDDHHMMSSZ | Use for dates up to and including 2049. |
| generalTime | | YYYYMMDDHHMMSSZ | Use for dates after 2049 |
| notAfter | | (issue date + up to 13 months) | The notAfter time MUST not be after the PIV card exp. date. |
| utcTime | | YYMMDDHHMMSSZ | Use for dates up to and including 2049. |
| generalTime | | YYYYMMDDHHMMSSZ | Use for dates after 2049 |
| **subject** | | | |
| RelativeDistinguishedName | | | |
| countryName (2.5.4.6) | | US | Required when multiple DC are NOT used |
| domainComponent (0.9.2342.19200300.100.1.25) | | com | If not multiple DC, then single Country is permitted i.e.C=US |
| domainComponent (0.9.2342.19200300.100.1.25) | | DigiCert-Grid or DigiCertGrid | If not multiple DC, then single Country is permitted i.e.C=US |
| organizationName (2.5.4.10) | | If C=US, then O=DigiCert Grid, else optional | Optional except where Country is used, then compulsory to at least use use "O=DigiCert Grid" |
| organizationalUnitName (2.5.4.11) | | People | OU= People |
| commonName (2.5.4.3) | | (name of subject) + [Unique ID if required] | name of subject, unique ID may be used if multiple separate subjects have the same name |
| **subjectPublicKeyInfo** | | | |
| algorithm | | | |
| AlgorithmIdentifier | | | Public key algorithm associated with the public key. |
| algorithm | | 1.2.840.113549.1.1.1 | RSA Encryption |
| RSAParameters | | NULL | For RSA, parameters field is populated with NULL. |
| subjectPublicKey | | BIT STRING | Modulus of at least 2048 bits. |
| **required extensions** | | | |
| **authorityKeyIdentifier** | FALSE | OCTET STRING | Derived using the SHA-1 hash of the public key. |
| **subjectKeyIdentifier** | FALSE | OCTET STRING | Derived using the SHA-1 hash of the public key. |
| **keyUsage** | TRUE | | |
| digitalSignature | | 1 | must be asserted. |
| nonRepudiation | | 0 | |
| keyEncipherment | | 1 | Must be asserted |
| dataEncipherment | | 1 | May be asserted |
| keyAgreement | | 0 | |
| keyCertSign | | 0 | |
| cRLSign | | 0 | |
| encipherOnly | | 0 | |
| decipherOnly | | 0 | |
| **basicConstraints (2.5.29.19)** | **TRUE** | | |
| End Entity | | Y | |
| pathLenConstraint | | None | |
| **certificatePolicies** | FALSE | | |
| PolicyInformation | | | |
| policyIdentifier | | 1.2.840.113612.5.2.2.1 | IGTF Classic OID |
| policyIdentifier | | 2.16.840.1.114412.4.31.1 | DigiCert Grid Classic Public Trust Client |
| policyIdentifier | | 1.2.840.113612.5.2.3.3.3 | IGTF 1SCP Natural Person |
| **cRLDistributionPoints (2.5.29.31)** | FALSE | | |
| DistributionPointName | | | |
| fullName | | http://crl3.digicert.com/DigiCertGridTrustCA.crl | |
| DistributionPointName | | | |
| fullName | | http://crl4.digicert.com/DigiCertGridTrustCA.crl | |

| | | | |
|---|---|---|---|
| **authorityInfoAccess (1.3.6.1.5.5.7.1.1)** | FALSE | | |
| accessMethod | | On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) | |
| accessLocation | | http://ocsp.digicert.com | GeneralName (uniformResourceIdentifier) |
| accessMethod | | id-ad-calssuers (1.3.6.1.5.5.7.48.2) | |
| accessLocation | | http://cacerts.digicert.com/DigiCertGridTrustCA.crt | GeneralName (uniformResourceIdentifier) |
| **extKeyUsage** | FALSE | | |
| keyPurposeID | | 1.3.6.1.5.5.7.3.2 | Client Authentication |
| | | Optional (1.3.6.1.5.5.7.3.4) | Secure Email |
| **subjectAltName** | FALSE | | |
| rfc822Name | | IA5String | Electronic mail address of the subscriber |
| **Signature** | | | |
| signatureAlgorithm | | 1.2.840.113549.1.1.5 or 1.2.840.113549.1.1.11 | sha1withRSAEncryption or Sha256WithRSAEncryption |
| **signature** | | | |

**NOTE: GFD125 compliant, for IGTF Accreditation**