Non Public Root: DigiCert Grid Root CA

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		02 61 38 7c 37 b4 39 a5 84 fa a1 52 52 da c8 ea	
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.
domainComponent (0.9.2342.19200300.100.1.25)		com	
domainComponent (0.9.2342.19200300.100.1.25)		DigiCert-Grid	
organizationName (2.5.4.10)		DigiCert Grid	
commonName (2.5.4.3)		DigiCert Grid Root CA	
validity			
notBefore Time		Wednesday, December 07, 2011 5:00:00 AM	utcTime - YYMMDDHHMMSSZ
notAfter Time		Sunday, December 07, 2036 5:00:00 AM	utcTime - YYMMDDHHMMSSZ
subject			
RelativeDistinguishedName			Matches Issuer DN.
domainComponent (0.9.2342.19200300.100.1.25)		com	
domainComponent (0.9.2342.19200300.100.1.25)		DigiCert-Grid	
organizationName (2.5.4.10)		DigiCert Grid	
commonName (2.5.4.3)		DigiCert Grid 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		key bits… (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		None	
subjectKeyIdentifier (2.5.29.14)		3d c8 d4 b3 b9 a1 77 50 97 50 11 50 a8 39 e5 1c 53 63 c6 70	
authorityKeyIdentifier (2.5.29.35)		keyID=3d c8 d4 b3 b9 a1 77 50 97 50 11 50 a8 39 e5 1c 53 63 c6 70	
Signature			
signatureAlgorithm		1.2.840.113549.1.1.5	sha1withRSAEncryption
signature		Signature bits	

NOTE: GFD125 compliant, for IGTF Accreditation

Non Public Trust subCA: DigiCert Grid CA-1

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		02 9e ff d2 4f 0b 7d 23 99 35 9b 9b 1f d6 f3 de	
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			
domainComponent (0.9.2342.19200300.100.1.25)		com	
domainComponent (0.9.2342.19200300.100.1.25)		DigiCert-Grid	
organizationName (2.5.4.10)		DigiCert Grid	
commonName (2.5.4.3)		DigiCert Grid Root CA	
validity			
notBefore Time		Wednesday, December 07, 2011 5:01:00 AM	utcTime - YYMMDDHHMMSSZ
notAfter Time		Monday, December 07, 2026 5:01:00 AM	utcTime - YYMMDDHHMMSSZ
subject			
RelativeDistinguishedName			
domainComponent (0.9.2342.19200300.100.1.25)		com	
domainComponent (0.9.2342.19200300.100.1.25)		DigiCert-Grid	
organizationName (2.5.4.10)		DigiCert Grid	
commonName (2.5.4.3)		DigiCert Grid CA-1	
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)	
accessLocation		http://cacerts.digicert.com/aiaDigiCertGridCA-1.p7c	GeneralName (uniformResourceIdentifier)
cRLDistributionPoints (2.5.29.31)	FALSE		
DistributionPointName			
fullName		http://crl3.digicert.com/DigiCertGridRootCA.crl	
DistributionPointName			
fullName		http://crl4.digicert.com/DigiCertGridRootCA.crl	
extendedKeyUsage (2.5.29.37)	FALSE	Not Present	
subjectKeyIdentifier (2.5.29.14)	FALSE	ef b0 75 9d 68 31 d1 e4 f7 2a 89 82 53 9d 39 77 68 2e 20 51	
authorityKeyIdentifier (2.5.29.35)	FALSE	KeyID=3d c8 d4 b3 b9 a1 77 50 97 50 11 50 a8 39 e5 1c 53 63 c6 70	
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 - Grid-Only 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			
domainComponent (0.9.2342.19200300.100.1.25)		com	
domainComponent (0.9.2342.19200300.100.1.25)		DigiCert-Grid	
organizationName (2.5.4.10)		DigiCert Grid	
commonName (2.5.4.3)		DigiCert Grid CA-1	
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		2.16.840.1.114412.31.1.1.1	DigiCert Grid Classic Host Grid-Only 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/DigiCertGridCA-1.crl	
DistributionPointName			
fullName		http://crl4.digicert.com/DigiCertGridCA-1.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/DigiCertGridCA-1.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 - Grid-Only 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			
domainComponent (0.9.2342.19200300.100.1.25)		com	
domainComponent (0.9.2342.19200300.100.1.25)		DigiCert-Grid	
organizationName (2.5.4.10)		DigiCert Grid	
commonName (2.5.4.3)		DigiCert Grid CA-1	
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		2.16.840.1.114412.31.4.1.1	DigiCert Grid Classic Grid-Only 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/DigiCertGridCA-1.crl	
DistributionPointName			

fullName		http://crl4.digicert.com/DigiCertGridCA-1.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/DigiCertGridCA-1.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

Grid Robot : Automated Grid Robot Profile - Grid-Only 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 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			
domainComponent (0.9.2342.19200300.100.1.25)		com	
domainComponent (0.9.2342.19200300.100.1.25)		DigiCert-Grid	
organizationName (2.5.4.10)		DigiCert Grid	
commonName (2.5.4.3)		DigiCert Grid CA-1	
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)		Robot	OU= Robot
commonName (2.5.4.3)		"Robot/"+ (FQDN)	Service Robots allowed
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	
certificatePolicies	FALSE		
PolicyInformation			
policyIdentifier		1.2.840.113612.5.2.2.1	IGTF Classic OID
policyIdentifier		2.16.840.1.114412.31.1.1.1	DigiCert Grid Classic Host Grid-Only Trust
policyIdentifier		1.2.840.113612.5.2.3.3.1	IGTF 1SCP Robot or Auto Client
cRLDistributionPoints (2.5.29.31)	FALSE		
DistributionPointName			
fullName		http://crl3.digicert.com/DigiCertGridCA-1.crl	
DistributionPointName			
fullName		http://crl4.digicert.com/DigiCertGridCA-1.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/DigiCertGridCA-1.crt	GeneralName (uniformResourceIdentifier)
extKeyUsage	FALSE		
keyPurposeID		serverAuth (1.3.6.1.5.5.7.3.1)	Required for service robots
		clientAuth (1.3.6.1.5.5.7.3.2) - Optional	Optional for service robots
subjectAltName	FALSE		
dNSName		(IA5String)	Required
rfc822Name		(IA5String)	Required to identify person responsible for Robot
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