Non Public Root: DigiCert Grid TEST Root CA

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		unique random #	
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 TEST Root CA	
validity			
notBefore Time		(issue date)	utcTime - YYMMDDHHMMSSZ
notAfter Time		(issue date + 25 years)	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 TEST 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**	06	
digitalSignature		0	
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)		keyID	
authorityKeyIdentifier (2.5.29.35)		keyID=...keyID	
Signature			
signatureAlgorithm		1.2.840.113549.1.1.5	sha1withRSAEncryption
signature		Signature bits	

NOTE: GFD125 compliant

Non Public Trust TEST subCA: DigiCert Grid TEST CA-1

Field	Criticality Flag	Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		(unique random assigned by CA)	
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 TEST Root CA	
validity			
notBefore Time		(issue date)	utcTime - YYMMDDHHMMSSZ
notAfter Time		(issue date + 15 years)	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 TEST 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**	06	
digitalSignature		0	
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	
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.test.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.test.digicert.com/DigiCertGridTESTRootCA.p7c	GeneralName (uniformResourceIdentifier)
cRLDistributionPoints (2.5.29.31)	FALSE		This extension is required in all CA certificates and must
DistributionPointName			
fullName		http://crl3.test.digicert.com/DigiCertGridTESTRootCA.crl	
DistributionPointName			
fullName		http://crl4.test.digicert.com/DigiCertGridTESTRootCA.crl	

extendedKeyUsage (2.5.29.37)	FALSE	Not Present	
subjectKeyIdentifier (2.5.29.14)	FALSE	(keyID)	
authorityKeyIdentifier (2.5.29.35)	FALSE	keyID=…keyID	
Signature			
signatureAlgorithm		1.2.840.113549.1.1.5 or 1.2.840.113549.1.1.11	sha1withRSAEncryption or Sha256WithRSAEncryption
signature			

NOTE: GFD125 compliant

Grid Host : Grid Service or Host Certificate

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 TEST 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			
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	
keyEncipherment		1	Must be asserted
dataEncipherment		1	May be asserted
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		
PolicyInformation			
policyIdentifier		2.16.840.1.114412.99.4.31.1	DigiCert Grid Classic TEST OID
policyIdentifier		1.2.840.113612.5.2.3.2.1	IGTF 1SCP Host
cRLDistributionPoints (2.5.29.31)	FALSE		
DistributionPointName			
fullName		http://crl3.test.digicert.com/DigiCertGridTESTCA-1.crl	

DistributionPointName			
fullName		http://crl4.test.digicert.com/DigiCertGridTESTCA-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.test.digicert.com	GeneralName (uniformResourceIdentifier)
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	
accessLocation		http://cacerts.test.digicert.com/DigiCertGridTESTCA-1.p7c	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 - can be multiple FQDNs listed here to support virtual hosting
rfc822Name		Optional (IA5String)	Electronic mail address of the server/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

Grid Client : Dual Purpose Grid Certificate Profile

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 TEST 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			
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)	name of subject
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		2.16.840.1.114412.99.4.31.1	DigiCert Grid Classic TEST OID
policyIdentifier		1.2.840.113612.5.2.3.3.1	IGTF 1SCP Natural Person
cRLDistributionPoints (2.5.29.31)	FALSE		
DistributionPointName			
fullName		http://crl3.test.digicert.com/DigiCertGridTESTCA-1.crl	
DistributionPointName			
fullName		http://crl4.test.digicert.com/DigiCertGridTESTCA-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.test.digicert.com	GeneralName (uniformResourceIdentifier)
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	
accessLocation		http://cacerts.test.digicert.com/DigiCertGridTESTCA-1.p7c	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

Grid Robot : Automated Grid Client Profile

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 TEST 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			
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		2.16.840.1.114412.99.4.31.1	DigiCert Grid Classic TEST OID
policyIdentifier		1.2.840.113612.5.2.3.1.1	IGTF 1SCP Robot or Auto Client
cRLDistributionPoints (2.5.29.31)	FALSE		
DistributionPointName			
fullName		http://crl3.test.digicert.com/DigiCertGridTESTCA-1.crl	

DistributionPointName			
fullName		http://crl4.test.digicert.com/DigiCertGridTESTCA-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.test.digicert.com	GeneralName (uniformResourceIdentifier)
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	
accessLocation		http://cacerts.test.digicert.com/DigiCertGridTESTCA-1.p7c	GeneralName (uniformResourceIdentifier)
extKeyUsage	FALSE		
keyPurposeID		serverAuth (1.3.6.1.5.5.7.3.1)	Required
		clientAuth (1.3.6.1.5.5.7.3.2) - Optional	Optional for service robots
subjectAltName	FALSE		
dNSName		(IA5String)	Required
rfc822Name		Optional (IA5String)	Optional unless Client Auth is specified in EKU
Signature			
signatureAlgorithm		1.2.840.113549.1.1.5 or 1.2.840.113549.1.1.11	sha1withRSAEncryption or Sha256WithRSAEncryption
signature			

NOTE: GFD125 compliant