

Virginia Tech Middleware Server Certificate Profile

Field	Format	Criticality Flag	Value or Content	Comments
Certificate				
tbsCertificate				----- START OF FIELDS TO BE SIGNED (tbsCertificate) -----
version				
ExplicitVersionNumber	INTEGER		2	Value of "2" for Version3.
serialNumber				
CertificateSerialNumber	INTEGER		0	Unique Integer supplied by CA when signed
signature				
AlgorithmIdentifier				Must match Algorithm Identifier in Certificate:signatureAlgorithm field.
algorithm	OID		1:2:840:113549:1:1:5	Choice of following identifiers: 1:2:840:113549:1:1:5 for SHA-1WithRSAEncryption 1:2:840:113549:1:1:4 for md5withRSAEncryption 1:2:840:10040:4:3 for id-dsa-with-sha-1
parameters	ANY			NULL type for RSA, DomainParameters for DSA, as described in RFC3280
issuer				
Name				X.500 Distinguished name of the issuer of the certificate.
RDNSequence				
RelativeDistinguishedName	SET OF			Sample DN: DC=edu,DC=vt,C=US,O=Virginia Polytechnic Institute and State University,CN=Virginia Tech Middleware CA
AttributeTypeAndValue	SEQUENCE			Sequence of AttributeTypes and AttributeValues
AttributeType	OID		0.9.2342.19200300.100.1.25	DC=edu
AttributeValue	uft8String			
AttributeTypeAndValue				
AttributeType	OID		0.9.2342.19200300.100.1.25	DC=vt
AttributeValue	uft8String			
AttributeTypeAndValue				
AttributeType	OID		2.5.4.6	C=US
AttributeValue	uft8String			
AttributeTypeAndValue				
AttributeType	OID		2.5.4.10	O=Virginia Polytechnic Institute and State University
AttributeValue	uft8String			
AttributeTypeAndValue				
AttributeType	OID		2.5.4.3	CN=Virginia Tech Middleware CA

Virginia Tech Middleware Server Certificate Profile

Field	Format	Criticality Flag	Value or Content	Comments
AttributeValue	uft8String			
AttributeTypeAndValue	SEQUENCE			Sequence of AttributeTypes and AttributeValues
validity	SEQUENCE			
notBefore				1 year certificate (365 days)
Time	CHOICE			CHOICE OF ONE of the following forms:
utcTime				
UTCTime	YYMMDDHHMMSSZ			Use for dates up to and including 2049.
notAfter				
Time	CHOICE			CHOICE OF ONE of the following forms:
utcTime				
UTCTime	YYMMDDHHMMSSZ			Use for dates up to and including 2049.
subject				
Name				X.500 Distinguished name of the owner of the certificate.
RDNSequene				(DC=edu,DC=vt,C=US,ST=Virginia,L=Blacksburg,O=Virginia Polytechnic Institute and State University,OU=Servers) are required attributes and values
RelativeDistinguishedName	SET OF			Sample DN: DC=edu,DC=vt,C=US,ST=Virginia,L=Blacksburg,O=Virginia Polytechnic Institute and State University, OU=Servers, OU=Servers, OU=34, CN=edid_server
AttributeTypeAndValue	SEQUENCE			Sequence of AttributeTypes and AttributeValues
AttributeType	OID		0.9.2342.19200300.100.1.25	DC=edu
AttributeValue	uft8String			
AttributeTypeAndValue				
AttributeType	OID		0.9.2342.19200300.100.1.25	DC=vt
AttributeValue	uft8String			
AttributeTypeAndValue				
AttributeType	OID		2.5.4.6	C=US
AttributeValue	uft8String			
AttributeTypeAndValue				
AttributeType	OID		2.5.4.8	ST=Virginia
AttributeValue	uft8String			
AttributeTypeAndValue				
AttributeType	OID		2.5.4.7	L=Blacksburg
AttributeValue	uft8String			

Virginia Tech Middleware Server Certificate Profile

Field	Format	Criticality Flag	Value or Content	Comments
AttributeTypeAndValue				
AttributeType	OID		2.5.4.10	O=Virginia Polytechnic Institute and State University
AttributeValue	uft8String			
AttributeTypeAndValue				
AttributeType	OID		2.5.4.11	OU=Middleware-Server is assigned by the CA when signed
AttributeValue	uft8String			
AttributeTypeAndValue				
AttributeType	OID		2.5.4.11	OU=x where x is the certificate serial number, a unique integer assigned by the CA when signed
AttributeValue	uft8String			
AttributeTypeAndValue				
AttributeType	OID		2.5.4.3	CN=server service name (Required attribute, User defined value)
AlgorithmIdentifier				Public key algorithm used.
algorithm	OID		1:2:840:113549:1:1:1	Choice of following identifiers: 1:2:840:113549:1:1:1 for RSA Encryption 1:2:840:10040:4:1 for Digital Signature Algorithm
parameters	ANY			NULL type for RSA, DomainParameters for DSA, as described in RFC3280
subjectPublicKey	BIT STRING			The detail is defined in RFC3280.
extensions				
AuthorityKeyIdentifier	CHOICE	FALSE	extnID {id-ce 35}	See RFC 3280. CHOICE of either keyIdentifier or (authorityCertIssuer and authorityCertSerialNumber) . Please remove unused formats.
keyIdentifier	OCTET STRING			Derived using the SHA-1 hash of the public key.
SubjectKeyIdentifier		FALSE	extnID {id-ce 14}	
keyIdentifier	OCTET STRING			Derived using the SHA-1 hash of the public key.
KeyUsage	BIT STRING	FALSE	extnID {id-ce 15}	Any subset combination of the key usages is also valid.
digitalSignature	(0)		1	
nonRepudiation	(1)		1	
keyEncipherment	(2)		1	
dataEncipherment	(3)		1	
keyAgreement	(4)		0	
keyCertSign	(5)		0	
cRLSign	(6)		0	

Virginia Tech Middleware Server Certificate Profile

Field	Format	Criticality Flag	Value or Content	Comments
encipherOnly	(7)		0	
decipherOnly	(8)		0	
certificatePolicies		FALSE	extnID {id-ce 32}	Criticality is dependent on the method of implementing certificate revocation.
PolicyInformation				
policyIdentifier	OID		1.3.6.1.4.1.6760.5.2.2.1.1	Refers to Certificate Level of Assurance LOA1
policyIdentifier	OID		1.3.6.1.4.1.6760.5.2.2.2.1	Refers to Certificate Level of Assurance LOA2 (not used)
policyIdentifier	OID		1.3.6.1.4.1.6760.5.2.2.3.1	Refers to Certificate Level of Assurance LOA3
policyIdentifier	OID		1.3.6.1.4.1.6760.5.2.2.4.1	Refers to Certificate Level of Assurance LOA4 (not used)
policyIdentifier	OID		1.3.6.1.4.1.6760.5.2.2.5.1	Refers to Certificate Level of Assurance LOA5 (not used)
policyQualifiers				OPTIONAL. Please remove if unused. If used, PolicyQualifierInfo may be multiply defined.If only one PolicyQualifierInfo is used, please remove the other PolicyQualifierInfo.
PolicyQualifierInfo				
policyQualifierId			{id-qt-cps}	Certificate Policy Statement (CP)
CPSuri	IA5String		http://www.pki.vt.edu/vtmw/cps/	URI for retrieving the CP.
BasicConstraints		FALSE	extnID {id-ce 19}	
cA	BOOLEAN		FALSE	Default is False.
pathLenConstraint	INTEGER			Meaningful only if cA is TRUE
ExtKeyUsageSyntax		FALSE	extnID {id-ce 37}	multiple KeyPurposeId may be used.
KeyPurposeId	OID		serverAuth	One or more of id-kp-serverAuth, id-kp-clientAuth, id-kp-codeSigning, id-kp-emailProtection, id-kp-ipsecEndSystem, id-kp-ipsecTunnel, id-kp-ipsecUser, id-kp-timeStamping
cRLDistributionPoints		FALSE		Criticality is dependent on the method of implementing certificate revocation.
CRLDistPointsSyntax				multiple DistriubtionPoint may be used.
DistributionPoint				
distributionPoint				OPTIONAL. Please remove if unused.
fullName				
GeneralNames	SEQUENCE			multiple GeneralName may be used.
GeneralName	CHOICE			
uniformResourceIdentifier	IA5String		https://vtmwra.eprov.iad.vt.edu/crl/cacrl.crl	
				----- END OF FIELDS TO BE SIGNED (tbsCertificate) -----
signatureAlgorithm				

Virginia Tech Middleware Server Certificate Profile

Field	Format	Criticality Flag	Value or Content	Comments
AlgorithmIdentifier				Must match Algorithm Identifier in Certificate:tbsCertificate:signature field.
algorithm	OID		1:2:840:113549:1:1:5	Choice of following identifiers: 1:2:840:113549:1:1:5 for SHA-1WithRSAEncryption 1:2:840:113549:1:1:4 for md5withRSAEncryption 1:2:840:10040:4:3 for id-dsa-with-sha-1
parameters	ANY			NULL type for RSA, DomainParameters for DSA, as described in RFC3280
signatureValue	BIT STRING			(Calculated)