

## Virginia Tech Middleware CA Profile

Field	Format	Criticality Flag	Value or Content	Comments
Certificate				
tbsCertificate				----- START OF FIELDS TO BE SIGNED (tbsCertificate) -----
<b>version</b>				
ExplicitVersionNumber	INTEGER		2	Value of "2" for Version3.
<b>serialNumber</b>				
CertificateSerialNumber	INTEGER		4	Unique Integer supplied by CA when signed
<b>signature</b>				
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
<b>issuer</b>				
Name				X.500 Distinguished name of the issuer of the certificate.
RDNSSequence				
RelativeDistinguishedName	SET OF			Sample DN: C=US,ST=Virginia,L=Blacksburg,O=Virginia Tech Root
AttributeTypeAndValue	SEQUENCE			Sequence of AttributeTypes and AttributeValues
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			
AttributeTypeAndValue				
AttributeType	OID		2.5.4.10	O=Virginia Tech Root CA
AttributeValue	uft8String			
<b>validity</b>	SEQUENCE			
<b>notBefore</b>				10 year certificate (3650 days)
Time	CHOICE			<b>CHOICE OF ONE of the following forms:</b>

## Virginia Tech Middleware CA Profile

Field	Format	Criticality Flag	Value or Content	Comments
utcTime				
UTCTime	YYMMDDHHMMSSZ			Use for dates up to and including 2049.
<b>notAfter</b>				
Time	CHOICE			<b>CHOICE OF ONE of the following forms:</b>
utcTime				
UTCTime	YYMMDDHHMMSSZ			Use for dates up to and including 2049.
<b>subject</b>				
Name				X.500 Distinguished name of the owner 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
AttributeValue	uft8String			
<b>subjectPublicKeyInfo</b>				
<b>algorithm</b>				
AlgorithmIdentifier				Public key algorithm used.
algorithm	OID		1:2:840:113549:1:1:1	<b>Choice of following identifiers:</b>
				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

## Virginia Tech Middleware CA Profile

Field	Format	Criticality Flag	Value or Content	Comments
<b>subjectPublicKey</b>	BIT STRING			The detail is defined in RFC3280.
<b>extensions</b>				
<b>AuthorityKeyIdentifier</b>	<b>CHOICE</b>	FALSE	extnID {id-ce 35}	See RFC 3280. CHOICE of either <b>keyIdentifier</b> or ( <b>authorityCertIssuer</b> and <b>authorityCertSerialNumber</b> ) . Please remove unused formats.
keyIdentifier	OCTET STRING			Derived using the SHA-1 hash of the public key.
<b>SubjectKeyIdentifier</b>		FALSE	extnID {id-ce 14}	
keyIdentifier	OCTET STRING			Derived using the SHA-1 hash of the public key.
<b>KeyUsage</b>	BIT STRING	FALSE	extnID {id-ce 15}	Any subset combination of the key usages is also valid.
digitalSignature	(0)		0	
nonRepudiation	(1)		0	
keyEncipherment	(2)		0	
dataEncipherment	(3)		0	
keyAgreement	(4)		0	
keyCertSign	(5)		1	
cRLSign	(6)		1	
encipherOnly	(7)		0	
decipherOnly	(8)		0	
<b>certificatePolicies</b>		FALSE	extnID {id-ce 32}	Criticality is dependent on the method of implementing certificate revocation.
PolicyInformation				
policyIdentifier	OID		1.3.6.1.4.1.6760.5.2.1.1.1	Refers to the CP for this CA
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		<a href="http://www.pki.vt.edu/vtmw/cps/">http://www.pki.vt.edu/vtmw/cps/</a>	URI for retrieving the CP.
<b>BasicConstraints</b>		TRUE	extnID {id-ce 19}	
cA	BOOLEAN		TRUE	Default is False.
pathLenConstraint	INTEGER			Meaningful only if cA is TRUE
<b>cRLDistributionPoints</b>		FALSE	extnID {id-ce 31}	Criticality is dependent on the method of implementing certificate revocation.
CRLDistPointsSyntax				multiple DistirubionPoint may be used.
DistributionPoint				

## Virginia Tech Middleware CA Profile

Field	Format	Criticality Flag	Value or Content	Comments
distributionPoint				OPTIONAL. Please remove if unused.
fullName				
GeneralNames	SEQUENCE			multiple GeneralName may be used.
GeneralName	CHOICE			
uniformResourceIdentifier	IA5String		<a href="http://www.pki.vt.edu/rootca/crl/cacrl.crl">http://www.pki.vt.edu/rootca/crl/cacrl.crl</a>	
----- END OF FIELDS TO BE SIGNED (tbsCertificate) -----				
signatureAlgorithm				
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)