

## Virginia Tech User Certificate 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 Version 3.
<b>serialNumber</b>				
CertificateSerialNumber	INTEGER		x	where x is a 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 RFC2459
<b>issuer</b>				
Name				X.500 Distinguished name of the issuer of the certificate.
RDNSequence				C= ; O= ; OU= ; and CN= are recommended
RelativeDistinguishedName	SET OF			Multiple AttributeTypeandValue may be used. Please remove unused types.
AttributeTypeAndValue	SEQUENCE			Sequence of AttributeTypes and AttributeValues
AttributeType	OID		DC=	DC=edu
AttributeValue	uft8String			
AttributeTypeAndValue				
AttributeType	OID		DC=	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 User CA

## Virginia Tech User Certificate Profile

Field	Format	Criticality Flag	Value or Content	Comments
AttributeValue	uft8String			
<b>validity</b>	<b>SEQUENCE</b>			
<b>notBefore</b>				2 year certificate (730 days)
Time	CHOICE			<b>CHOICE OF ONE of the following forms:</b>
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				<b>C= ; O= ; OU= ; CN= ; and UID= are recommended</b>
RelativeDistinguishedName	SET OF			Multiple AttributeTypeandValue may be used. Please remove unused types.
AttributeTypeAndValue	SEQUENCE			Sequence of AttributeTypes and AttributeValues
AttributeType	OID		DC=	DC=edu
AttributeValue	uft8String			
AttributeTypeAndValue				
AttributeType	OID		DC=	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		0.9.2342.19200300.100.1.1	uid=<user unique university UID from ED-ID>
AttributeValue	uft8String			
AttributeTypeAndValue				
AttributeType	OID		2.5.4.3	CN=<user legal name form ED-ID>
AttributeValue	uft8String			

## Virginia Tech User Certificate Profile

Field	Format	Criticality Flag	Value or Content	Comments
AttributeTypeAndValue				
AttributeType	OID		2.5.4.5	serialNumber=<a unique integer assigned by CA when signed>
AttributeValue	uft8String			
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 RFC2459
subjectPublicKey	BIT STRING			The detail is defined in RFC2459.
<b>extensions</b>				
<b>AuthorityKeyIdentifier</b>	<b>CHOICE</b>	FALSE	extnID {id-ce 35}	See RFC 2459. 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)		1	Digital Signature
nonRepudiation	(1)		1	Non-Repudiation
keyEncipherment	(2)		1	Key Encipherment
dataEncipherment	(3)		0	
keyAgreement	(4)		0	
keyCertSign	(5)		0	
cRLSign	(6)		0	
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		1.3.6.1.4.1.6760.5.2.2.1.1	Test Assurance Level OID
policyIdentifier	OID		1.3.6.1.4.1.6760.5.2.2.2.1	Rudimentary Assurance Level OID
policyIdentifier	OID		1.3.6.1.4.1.6760.5.2.2.3.1	Basic Assurance Level OID
policyIdentifier	OID		1.3.6.1.4.1.6760.5.2.2.4.1	Medium Assurance Level OID

## Virginia Tech User Certificate Profile

Field	Format	Criticality Flag	Value or Content	Comments
policyIdentifier	OID		1.3.6.1.4.1.6760.5.2.2.5.1	High Assurance Level OID
PolicyQualifierInfo				
CPSuri	IA5String		<a href="http://www.pki.vt.edu/vtuca/cps/">http://www.pki.vt.edu/vtuca/cps/</a>	URI for retrieving the CPS.
<b>SubjectAltName</b>		FALSE	extnID {id-ce 17}	This extension need not appear in all certificates.
GeneralNames	SEQUENCE			Multiple GeneralName may be used. Please remove unused types.
GeneralName	CHOICE			CHOICE of ONE of (otherName, rfc822Name, dNSName, directoryName, ediPartyName, uniformResourceIdentifier, iPAddress)
rfc822Name	IA5String		<a href="mailto:PID@vt.edu">PID@vt.edu</a>	where PID is the university assigned Personal ID
<b>BasicConstraints</b>		FALSE	extnID {id-ce 19}	
CA	BOOLEAN		FALSE	Default is False.
<b>ExtKeyUsageSyntax</b>		FALSE	extnID {id-ce 37}	multiple KeyPurposeID may be used.
KeyPurposeID	OID		1.3.6.1.5.5.7.3.2	Web Client Authentication
KeyPurposeID	OID		1.3.6.1.5.5.7.3.4	E-mail Protection
KeyPurposeID	OID		1.3.6.1.4.1.311.20.2.2	Microsoft Smartcard Login
KeyPurposeID	OID		Client Authentication	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
<b>cRLDistributionPoints</b>		FALSE		Criticality is dependent on the method of implementing certificate revocation.
CRLDistPointsSyntax				multiple DistirubionPoint may be used.
DistributionPoint				
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/vtuca/crl/cacrl.crl">http://www.pki.vt.edu/vtuca/crl/cacrl.crl</a>	
----- END OF FIELDS TO BE SIGNED (tbsCertificate) -----				

### Virginia Tech User Certificate Profile

Field	Format	Criticality Flag	Value or Content	Comments
signatureAlgorithm				
AlgorithmIdentifier				Must match Algorithm Identifier in Certificate:tlsCertificate: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 RFC2459
signatureValue	BIT STRING			(Calculated)