

## Certificate

<a href="https://columbia.edu">columbia.edu</a>	InCommon RSA Server CA	USERTrust RSA Certification Authority
---	------------------------	---------------------------------------

<b>Subject Name</b>	
<b>Country</b>	US
	10027
<b>State/Province</b>	New York
<b>Locality</b>	New York
	116th Street and Broadway
<b>Organization</b>	Columbia University
<b>Organizational Unit</b>	Information Technology
<b>Common Name</b>	columbia.edu
<b>Issuer Name</b>	
<b>Country</b>	US
<b>State/Province</b>	MI
<b>Locality</b>	Ann Arbor
<b>Organization</b>	Internet2
<b>Organizational Unit</b>	InCommon
<b>Common Name</b>	<a href="#">InCommon RSA Server CA</a>
<b>Validity</b>	
<b>Not Before</b>	1/1/2020, 7:00:00 PM (Eastern Standard Time)
<b>Not After</b>	1/1/2022, 6:59:59 PM (Eastern Standard Time)
<b>Subject Alt Names</b>	
<b>DNS Name</b>	columbia.edu
<b>DNS Name</b>	*.columbia.edu
<b>Public Key Info</b>	
<b>Algorithm</b>	RSA
<b>Key Size</b>	2048
<b>Exponent</b>	65537
<b>Modulus</b>	C0:33:DA:C2:98:DE:44:41:A2:F5:87:D3:3E:AD:30:88:03:34:2D:36:C9:59:EB:86:64:37:B2:B3:E...
<b>Miscellaneous</b>	
<b>Serial Number</b>	00:DC:96:95:D4:2C:DF:5E:DE:EA:4B:13:5C:F7:0D:B5:5A
<b>Signature Algorithm</b>	SHA-256 with RSA Encryption
<b>Version</b>	3
<b>Download</b>	<a href="#">PEM (cert)</a> <a href="#">PEM (chain)</a>
<b>Fingerprints</b>	
<b>SHA-256</b>	19:11:6C:AB:8D:DD:9B:61:FD:9D:E8:9B:AE:C8:5C:71:0F:13:F8:C4:C0:4C:C1:5C:CF:A4:1B:86:89:C
<b>SHA-1</b>	EB:F5:DD:2A:D3:00:6D:FD:38:E2:66:D9:26:CA:9E:21:84:88:E0:83
<b>Basic Constraints</b>	
<b>Certificate Authority</b>	No

**Key Usages****Purposes** Digital Signature, Key Encipherment**Extended Key Usages****Purposes** Server Authentication, Client Authentication**Subject Key ID****Key ID** 87:40:6A:E9:CB:35:68:4F:94:30:36:0F:38:AD:60:18:5C:4D:5F:4D**Authority Key ID****Key ID** 1E:05:A3:77:8F:6C:96:E2:5B:87:4B:A6:B4:86:AC:71:00:0C:E7:38**CRL Endpoints****Distribution Point** <http://crl.incommon-rsa.org/InCommonRSAServerCA.crl>**Authority Info (AIA)****Location** [http://crt.usertrust.com/InCommonRSAServerCA\\_2.crt](http://crt.usertrust.com/InCommonRSAServerCA_2.crt)**Method** CA Issuers**Location** <http://ocsp.usertrust.com>**Method** Online Certificate Status Protocol (OCSP)**Certificate Policies****Policy** Statement Identifier ( 1.3.6.1.4.1 )**Value** 1.3.6.1.4.1.5923.1.4.3.1.1**Qualifier** Practices Statement ( 1.3.6.1.5.5.7.2.1 )**Value** [https://www.incommon.org/cert/repository/cps\\_ssl.pdf](https://www.incommon.org/cert/repository/cps_ssl.pdf)**Policy** Certificate Type ( 2.23.140.1.2.2 )**Value** Organization Validation**Embedded SCTs****Log ID** 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:4**Name** Google "Xenon2022"**Signature Algorithm** SHA-256 ECDSA**Version** 1**Timestamp** 1/2/2020, 1:58:59 PM (Eastern Standard Time)**Log ID** 6F:53:76:AC:31:F0:31:19:D8:99:00:A4:51:15:FF:77:15:1C:11:D9:02:C1:00:29:06:8D:B2:08:9A:37:D**Name** Sectigo (Comodo) "Mammoth" CT**Signature Algorithm** SHA-256 ECDSA**Version** 1**Timestamp** 1/2/2020, 1:58:59 PM (Eastern Standard Time)**Log ID** 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2**Name** DigiCert Yeti2022**Signature Algorithm** SHA-256 ECDSA**Version** 1**Timestamp** 1/2/2020, 1:58:59 PM (Eastern Standard Time)

# Certificate

columbia.edu	<a href="#">InCommon RSA Server CA</a>	USERTrust RSA Certification Authority
--------------	--	---------------------------------------

**Subject Name**

**Country** US  
**State/Province** MI  
**Locality** Ann Arbor  
**Organization** Internet2  
**Organizational Unit** InCommon  
**Common Name** InCommon RSA Server CA

**Issuer Name**

**Country** US  
**State/Province** New Jersey  
**Locality** Jersey City  
**Organization** The USERTRUST Network  
**Common Name** [USERTrust RSA Certification Authority](#)

**Validity**

**Not Before** 10/5/2014, 8:00:00 PM (Eastern Standard Time)  
**Not After** 10/5/2024, 7:59:59 PM (Eastern Standard Time)

**Public Key Info**

**Algorithm** RSA  
**Key Size** 2048  
**Exponent** 65537  
**Modulus** 9C:1B:F1:BB:2F:7F:63:18:15:51:51:54:0F:9E:C5:4E:4D:10:58:FA:30:9B:17:29:90:E6:33:0C:AC:13...

**Miscellaneous**

**Serial Number** 47:20:D0:FA:85:46:1A:7E:17:A1:64:02:91:84:63:74  
**Signature Algorithm** SHA-384 with RSA Encryption  
**Version** 3  
**Download** [PEM \(cert\)](#) [PEM \(chain\)](#)

**Fingerprints**

**SHA-256** 0A:05:C4:62:75:63:90:DD:1F:1D:5D:D8:27:94:C3:00:F0:4B:E7:89:DC:E7:6D:7E:31:2F:79:0D:68:FI  
**SHA-1** F5:FB:01:DE:A6:E5:9C:A6:DD:05:70:54:F4:A3:FF:72:DD:E1:D5:C6

**Basic Constraints**

**Certificate Authority** Yes

**Key Usages**

**Purposes** Digital Signature, Certificate Signing, CRL Signing

**Extended Key Usages**

**Purposes** Server Authentication, Client Authentication

**Subject Key ID**

**Key ID** 1E:05:A3:77:8F:6C:96:E2:5B:87:4B:A6:B4:86:AC:71:00:0C:E7:38

**Authority Key ID**

**Key ID** 53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB

**CRL Endpoints**

**Distribution Point** <http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl>

**Authority Info (AIA)**

**Location** <http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt>

**Method** CA Issuers

**Location** <http://ocsp.usertrust.com>

**Method** Online Certificate Status Protocol (OCSP)

**Certificate Policies**

**Policy** Certificate Type ( 2.23.140.1.2.2 )

**Value** Organization Validation

# Certificate

columbia.edu	InCommon RSA Server CA	<a href="#">USERTrust RSA Certification Authority</a>
--------------	------------------------	---

**Subject Name**

**Country** US  
**State/Province** New Jersey  
**Locality** Jersey City  
**Organization** The USERTRUST Network  
**Common Name** USERTrust RSA Certification Authority

**Issuer Name**

**Country** US  
**State/Province** New Jersey  
**Locality** Jersey City  
**Organization** The USERTRUST Network  
**Common Name** USERTrust RSA Certification Authority

**Validity**

**Not Before** 1/31/2010, 7:00:00 PM (Eastern Standard Time)  
**Not After** 1/18/2038, 6:59:59 PM (Eastern Standard Time)

**Public Key Info**

**Algorithm** RSA  
**Key Size** 4096  
**Exponent** 65537  
**Modulus** 80:12:65:17:36:0E:C3:DB:08:B3:D0:AC:57:0D:76:ED:CD:27:D3:4C:AD:50:83:61:E2:AA:20:4D:0...

**Miscellaneous**

**Serial Number** 01:FD:6D:30:FC:A3:CA:51:A8:1B:BC:64:0E:35:03:2D  
**Signature Algorithm** SHA-384 with RSA Encryption  
**Version** 3  
**Download** [PEM \(cert\)](#) [PEM \(chain\)](#)

**Fingerprints**

**SHA-256** E7:93:C9:B0:2F:D8:AA:13:E2:1C:31:22:8A:CC:B0:81:19:64:3B:74:9C:89:89:64:B1:74:6D:46:C3:D4  
**SHA-1** 2B:8F:1B:57:33:0D:BB:A2:D0:7A:6C:51:F7:0E:E9:0D:DA:B9:AD:8E

**Basic Constraints**

**Certificate Authority** Yes

**Key Usages**

**Purposes** Certificate Signing, CRL Signing

**Subject Key ID**

**Key ID** 53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB

**Subject Key ID**

**Key ID** 1E:05:A3:77:8F:6C:96:E2:5B:87:4B:A6:B4:86:AC:71:00:0C:E7:38

**Authority Key ID**

**Key ID** 53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB

**CRL Endpoints**

**Distribution Point** <http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl>

**Authority Info (AIA)**

**Location** <http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt>

**Method** CA Issuers

**Location** <http://ocsp.usertrust.com>

**Method** Online Certificate Status Protocol (OCSP)

**Certificate Policies**

**Policy** Certificate Type ( 2.23.140.1.2.2 )

**Value** Organization Validation