<table>
<thead>
<tr>
<th>Subject Name</th>
<th>InCommon RSA Server CA</th>
<th>USERTrust RSA Certification Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Country</strong></td>
<td>US</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10027</td>
<td></td>
</tr>
<tr>
<td><strong>State/Province</strong></td>
<td>New York</td>
<td></td>
</tr>
<tr>
<td><strong>Locality</strong></td>
<td>New York</td>
<td></td>
</tr>
<tr>
<td></td>
<td>116th Street and Broadway</td>
<td></td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>Columbia University</td>
<td></td>
</tr>
<tr>
<td><strong>Organizational Unit</strong></td>
<td>Information Technology</td>
<td></td>
</tr>
<tr>
<td><strong>Common Name</strong></td>
<td>columbia.edu</td>
<td></td>
</tr>
<tr>
<td><strong>Issuer Name</strong></td>
<td>US</td>
<td></td>
</tr>
<tr>
<td><strong>State/Province</strong></td>
<td>MI</td>
<td></td>
</tr>
<tr>
<td><strong>Locality</strong></td>
<td>Ann Arbor</td>
<td></td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>Internet2</td>
<td></td>
</tr>
<tr>
<td><strong>Organizational Unit</strong></td>
<td>InCommon</td>
<td></td>
</tr>
<tr>
<td><strong>Common Name</strong></td>
<td>InCommon RSA Server CA</td>
<td></td>
</tr>
<tr>
<td><strong>Validity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Not Before</strong></td>
<td>1/1/2020, 7:00:00 PM (Eastern Standard Time)</td>
<td></td>
</tr>
<tr>
<td><strong>Not After</strong></td>
<td>1/1/2022, 6:59:59 PM (Eastern Standard Time)</td>
<td></td>
</tr>
<tr>
<td><strong>Subject Alt Names</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DNS Name</strong></td>
<td>columbia.edu</td>
<td></td>
</tr>
<tr>
<td><strong>DNS Name</strong></td>
<td>*.columbia.edu</td>
<td></td>
</tr>
<tr>
<td><strong>Public Key Info</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Algorithm</strong></td>
<td>RSA</td>
<td></td>
</tr>
<tr>
<td><strong>Key Size</strong></td>
<td>2048</td>
<td></td>
</tr>
<tr>
<td><strong>Exponent</strong></td>
<td>65537</td>
<td></td>
</tr>
<tr>
<td><strong>Miscellaneous</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>00:DC:96:95:D4:2C:DF:5E:DE:EA:4B:13:5C:F7:0D:B5:5A</td>
<td></td>
</tr>
<tr>
<td><strong>Signature Algorithm</strong></td>
<td>SHA-256 with RSA Encryption</td>
<td></td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td><strong>Download</strong></td>
<td>PEM (cert) PEM (chain)</td>
<td></td>
</tr>
<tr>
<td><strong>Fingerprints</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Basic Constraints</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Certificate Authority</strong></td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Key Usages
Purposes  Digital Signature, Key Encipherment

Extended Key Usages
Purposes  Server Authentication, Client Authentication

Subject Key ID

Authority Key ID

CRL Endpoints
Distribution Point  http://crl.incommon-rsa.org/InCommonRSAServerCA.crl

Authority Info (AIA)
Location  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
Policy  Certificate Type (2.23.140.1.2.2)
Value  Organization Validation

Embedded SCTs
Name  Google "Xenon2022"
Signature Algorithm  SHA-256 ECDSA
Version  1
Timestamp  1/2/2020, 1:58:59 PM (Eastern Standard Time)
Name  Sectigo (Comodo) "Mammoth" CT
Signature Algorithm  SHA-256 ECDSA
Version  1
Timestamp  1/2/2020, 1:58:59 PM (Eastern Standard Time)
Name  DigiCert Yeti2022
Signature Algorithm  SHA-256 ECDSA
Version  1
Timestamp  1/2/2020, 1:58:59 PM (Eastern Standard Time)
Certificate

<table>
<thead>
<tr>
<th>columbia.edu</th>
<th>InCommon RSA Server CA</th>
<th>USERTrust RSA Certification Authority</th>
</tr>
</thead>
</table>

**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

**Miscellaneous**
- Signature Algorithm: SHA-384 with RSA Encryption
- Version: 3
- Download: PEM (cert) PEM (chain)

**Fingerprints**

**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

Authority Key ID

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

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

Miscellaneous
  Signature Algorithm  SHA-384 with RSA Encryption
  Version  3
  Download  PEM (cert) PEM (chain)

Fingerprints

Basic Constraints
  Certificate Authority  Yes

Key Usages
  Purposes  Certificate Signing, CRL Signing

Subject Key ID
Subject Key ID

Authority Key ID

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