Certificate

*.cs.columbia.edu	InCommon RSA Server CA	USERTrust RSA Certification Authority

Subject Name
Country US
10027
State/Province NY
Locality New York
116th Street and Broadway
Organization Columbia University
Organizational Unit Information Technology
Common Name *.cs.columbia.edu

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

Validity
Not Before 5/9/2018, 8:00:00 PM (Eastern Standard Time)
Not After 5/9/2020, 7:59:59 PM (Eastern Standard Time)

Subject Alt Names
DNS Name *.cs.columbia.edu

Public Key Info
Algorithm RSA
Key Size 2048
Exponent 65537
Modulus 9E:79:41:0D:61:68:74:09:D4:43:F3:BD:42:39:A5:CE:77:9A:40:39:BB:66:7B:B2:C3:C1:EC:AB:8...

Miscellaneous
Serial Number 4D:FC:EA:08:BB:13:5E:F9:1E:5F:89:86:41:B4:1C:59
Signature Algorithm SHA-256 with RSA Encryption
Version 3
Download PEM (cert) PEM (chain)

Fingerprints
SHA-256 40:01:2B:4C:F9:B7:8D:5C:3A:FF:47:5B:EE:47:00:D7:81:76:F1:E9:A6:81:A2:F0:FE:9C:40:5D:4C:C/
SHA-1 BD:7C:69:A7:21:EC:67:48:38:26:7F:BF:7E:CF:29:A5:3D:D0:1D:91

Basic Constraints
Certificate Authority No

Key Usages
Purposes Digital Signature, Key Encipherment

Extended Key Usages
Purposes Server Authentication, Client Authentication

Subject Key ID
Key ID C9:FE:C6:23:3F:0D:C3:C1:09:2F:D3:D3:0B:9A:ED:22:CF:07:82:D6

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
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
Log ID EE:4B:BD:B7:75:CE:60:BA:E1:42:69:1F:AB:E1:9E:66:A3:0F:7E:5F:B0:72:D8:83:00:C4:7B:89:7A:A8
Name Google “Rocketeer”
Signature Algorithm SHA-256 ECDSA
Version 1

Timestamp 5/10/2018, 10:43:58 AM (Eastern Standard Time)
Log ID 5E:A7:73:F9:DF:56:C0:E7:B5:36:48:7D:D0:49:E0:32:7A:91:9A:0C:84:A1:12:12:84:18:75:96:81:71:
Name Cloudflare “Nimbus2020”
Signature Algorithm SHA-256 ECDSA
Version 1

Timestamp 5/10/2018, 10:43:58 AM (Eastern Standard Time)
Log ID 55:81:D4:C2:16:90:36:01:4A:EA:0B:9B:57:3C:53:F0:C0:E4:38:78:70:25:08:17:2F:A3:AA:1D:07:13
Name Sectigo (Comodo) “Sabre” CT
Signature Algorithm SHA-256 ECDSA
Version 1

Timestamp 5/10/2018, 10:43:58 AM (Eastern Standard Time)

Certificate

*.cs.columbia.edu	InCommon RSA Server CA	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:F[
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

*.cs.columbia.edu	InCommon RSA Server CA	USERTrust RSA Certification Authority

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