crt.sh Certificate Search

Criteria   ID = '16994207368'

crt.sh ID	16994207368
Summary	Leaf certificate

Certificate Transparency

Log entries for this certificate:

Timestamp	Entry #	Log Operator	Log URL
2025-02-03 04:22:51 UTC	862661774	Google	https://ct.googleapis.com/logs/us1/argon2025h1

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Not Revoked	n/a	n/a	2025-03-22 15:50:29 UTC
CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

Certificate Fingerprints

SHA-256 D860DEB53EED9950CDE2BEE960BDFF48E585EA49578A0D2217CD96746E3997F1   SHA-1 010E1CA97AC8925303484A0ED0AA1E0E7DA7A34C

| ASN.1 | Certificate | Graph |
| Hierarchy | pv |

Hide metadata

Run linters using pkimetal

Download Certificate: PEM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:b7:96:74:59:72:77:1a:1b:2f:48:4d:cb:50:d6:f6:1d:75
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 295814)
            commonName                = R10
            organizationName          = Let's Encrypt
            countryName               = US
        Validity
            Not Before: Feb  3 03:24:20 2025 GMT
            Not After : May  4 03:24:19 2025 GMT
        Subject:
            commonName                = www.ev-bau.ch
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:a9:72:c2:0b:34:a3:56:43:e8:38:e6:b1:9f:0f:
                    e0:4e:db:34:95:7b:84:92:af:76:f9:2a:98:8a:d5:
                    fc:fb:26:f1:50:de:92:ac:43:5b:a8:7e:bf:03:6f:
                    76:ff:86:ce:a4:32:14:f5:ac:a2:22:9d:26:03:1a:
                    47:af:cb:fd:d2:71:80:b1:6e:e1:8b:6e:b8:62:04:
                    0e:d1:30:16:8c:b8:96:c2:28:e6:03:7c:25:97:92:
                    0e:57:71:11:4f:d7:7b:12:8c:53:4f:04:5d:5d:af:
                    88:4d:17:45:40:1f:72:f8:ec:9c:aa:e4:54:28:56:
                    ae:10:9a:3b:4c:fe:6e:ff:18:d6:89:21:59:e0:af:
                    3a:98:71:76:0f:02:65:6d:fd:26:96:46:77:3d:88:
                    1d:23:df:39:34:7e:dc:eb:bd:2a:45:db:dc:e3:44:
                    69:74:f5:8d:e0:4f:02:6d:64:f3:fa:5d:c8:01:d3:
                    6b:23:e3:5a:1d:36:66:6a:99:79:07:87:07:3b:2b:
                    ba:14:74:d8:3c:18:38:5c:bd:f0:e7:4d:db:c4:33:
                    ff:f3:c4:c2:ec:d6:d0:d8:27:98:c8:3e:a4:70:c2:
                    9f:9f:c1:a7:4c:2b:26:94:c2:c7:39:79:b6:57:38:
                    1a:9d:1d:3f:17:96:28:4b:76:ba:07:41:90:35:e7:
                    a2:1c:2e:d8:73:9d:5a:be:8c:5a:09:4a:86:57:f9:
                    b5:79:fd:be:1c:1e:8d:2c:ec:7f:ae:ec:06:b7:a2:
                    af:46:4c:99:8b:17:7a:a1:fd:8f:8a:e8:b5:18:9d:
                    06:db:b8:fd:49:64:b3:a0:94:2d:4e:4e:34:b6:4b:
                    e4:fe:91:61:a2:5f:d1:de:a8:2f:e2:c5:4e:48:a2:
                    ba:f5:4f:01:29:66:5a:68:2c:9c:fc:f3:58:7d:fa:
                    fa:2d:21:57:a3:a7:78:4b:0c:55:9a:52:3d:d0:66:
                    40:98:48:27:91:2d:6d:96:f7:00:c1:95:4e:6f:6c:
                    19:18:8d:96:d9:1f:7f:49:f9:dd:24:25:ec:c1:f4:
                    58:90:a3:f5:e7:b1:41:1a:14:45:f6:2b:db:50:8c:
                    a4:cc:fe:d1:2b:4e:f6:7e:dd:44:d2:77:fe:78:7f:
                    5b:dc:59:e6:77:e0:1c:80:0a:0e:e7:0a:80:e9:28:
                    04:4d:78:8c:8b:cc:cc:38:bd:e6:db:16:7e:46:c8:
                    78:3b:c3:55:c1:16:85:f8:78:82:ab:13:76:ce:f2:
                    87:24:d8:e1:98:ee:da:ff:78:88:ca:0c:24:e2:49:
                    9e:a6:d2:ba:11:d8:ad:c5:42:94:22:e7:55:73:9a:
                    3f:31:f0:1b:6b:a0:da:58:c9:db:7a:5a:42:68:20:
                    a1:bd:19
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                5A:F4:39:CD:35:22:89:2D:1B:3B:66:4F:C3:3C:60:6D:59:C7:26:EC
            X509v3 Authority Key Identifier:
                keyid:BB:BC:C3:47:A5:E4:BC:A9:C6:C3:A4:72:0C:10:8D:A2:35:E1:C8:E8

            Authority Information Access:
                OCSP - URI:http://r10.o.lencr.org
                CA Issuers - URI:http://r10.i.lencr.org/

            X509v3 Subject Alternative Name:
                DNS:ev-bau.ch
                DNS:www.ev-bau.ch
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1

            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log Name  : Let's Encrypt Oak 2025h1
                    Log ID    : A2:E3:0A:E4:45:EF:BD:AD:9B:7E:38:ED:47:67:77:53:
                                D7:82:5B:84:94:D7:2B:5E:1B:2C:C4:B9:50:A4:47:E7
                    Timestamp : Feb  3 04:22:50.540 2025 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:45:02:20:7B:2D:5A:FD:78:2D:FD:3B:19:60:32:12:
                                27:8B:55:F6:DC:61:B4:98:40:53:F2:AA:8E:80:4C:59:
                                47:81:5E:DA:02:21:00:FC:E7:F1:FD:D4:20:F0:AC:C1:
                                F4:1B:73:EA:12:C0:85:A0:A0:7C:29:55:1D:6B:FC:B5:
                                12:58:E5:F7:E8:66:0E
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log Name  : Sectigo Sabre 2025h1
                    Log ID    : E0:92:B3:FC:0C:1D:C8:E7:68:36:1F:DE:61:B9:96:4D:
                                0A:52:78:19:8A:72:D6:72:C4:B0:4D:A5:6D:6F:54:04
                    Timestamp : Feb  3 04:22:50.684 2025 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:45:02:20:1E:94:AF:FA:B3:FB:CF:0B:D1:FC:78:22:
                                AE:DB:CA:23:C9:C2:51:E0:93:4D:A1:07:DF:78:5F:67:
                                97:EC:CA:FE:02:21:00:8A:16:19:05:66:84:9D:61:46:
                                3E:87:28:B3:7A:44:12:8C:39:80:EA:D9:5D:56:B0:B9:
                                0D:8D:C5:67:79:42:63
        Signature Algorithm: sha256WithRSAEncryption
             73:ad:b2:5a:88:7e:00:3e:73:83:9d:80:66:b6:26:78:b1:ae:
             e3:c4:54:74:e9:bf:e8:7f:2a:34:0d:e7:f4:f8:b4:5b:41:62:
             3a:52:b4:de:d7:d9:02:56:72:2a:8a:6b:99:90:4b:3a:53:43:
             92:c9:ad:31:7f:e1:0b:0c:1e:0f:b2:14:5b:66:07:56:04:f1:
             b0:7f:bb:6c:51:33:02:25:31:86:7b:2d:24:52:70:fa:f1:09:
             22:32:6e:5d:1a:a4:43:1f:13:8a:5e:50:cb:2f:de:4b:47:55:
             0b:3a:fc:52:33:a2:70:15:cf:e0:6e:e3:a1:d6:71:be:bd:fd:
             7b:db:63:b6:15:7b:1c:b1:75:ae:fa:c1:ae:5a:c6:05:41:3f:
             1f:73:44:8c:58:f6:77:6d:7c:65:d2:84:55:a0:ce:96:d9:ad:
             46:1f:d9:d3:15:ee:c3:29:84:49:c8:49:f9:dd:18:72:2c:a0:
             a4:a7:b8:e9:49:e2:bb:93:59:c4:4d:89:d5:cc:b3:6b:17:92:
             52:d8:31:8f:da:42:66:a0:00:67:3a:dc:4b:cc:cb:d3:16:15:
             83:da:a9:01:13:07:dd:33:36:c0:6c:06:57:6f:41:1d:36:45:
             14:2e:cf:49:7f:22:4a:08:b7:fe:05:8e:f0:ea:95:c0:7d:ed:
             a2:e0:6f:83
```