**Microsec faulty certificate reports**

**Reference link:**

<https://crt.sh/?caid=1536&opt=cablint,zlint,x509lint&minNotBefore=2015-01-01>

**CA/B Forum lint**

**ERROR: Unallowed key usage for RSA public key (Key Agreement)  in 39 certificates**

|  |  |  |  |
| --- | --- | --- | --- |
| **crt.sh ID** | **Not Before** | **Not After** | **Subject Name** |
| [286773604](https://crt.sh/?id=286773604&opt=cablint) | 2016-11-24 | 2018-11-24 | C=HU, L=Budapest, O=Magyar Országos Közjegyzői Kamara, 2.5.4.97=VATHU-18000098-1-41, CN=avpn.mokk.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.391 |
| [287296655](https://crt.sh/?id=287296655&opt=cablint) | 2016-11-24 | 2018-11-24 | C=HU, L=Budapest, O=Magyar Országos Közjegyzői Kamara, CN=bvpn.mokk.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.1842 |
| [287280953](https://crt.sh/?id=287280953&opt=cablint) | 2016-11-24 | 2018-11-24 | C=HU, L=Budapest, O=Magyar Országos Közjegyzői Kamara, 2.5.4.97=VATHU-18000098-1-41, CN=fvpn.mokk.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2565 |
| [287284890](https://crt.sh/?id=287284890&opt=cablint) | 2016-08-29 | 2018-08-29 | C=HU, L=Budapest, O=Microsec zrt., 2.5.4.97=VATHU-23584497-2-41, CN=archivpob.e-szigno.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.89 |
| [286773327](https://crt.sh/?id=286773327&opt=cablint) | 2016-08-18 | 2018-08-18 | C=HU, L=Budapest, O=CONSEQUENCE Kft., 2.5.4.97=VATHU-13161497-2-41, CN=\*.consequence.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2469 |
| [286812259](https://crt.sh/?id=286812259&opt=cablint) | 2016-08-05 | 2018-08-05 | C=HU, L=Budapest, O=FŐTÁV Zrt., 2.5.4.97=VATHU-10941362-2-44, CN=tesztugyfelszolgalat.fotav.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2436 |
| [286408759](https://crt.sh/?id=286408759&opt=cablint) | 2016-06-30 | 2018-06-30 | C=HU, L=Budapest, O=Magyar Gáz Tranzit ZRt., OU=Vezérigazgatóság, CN=www.ip.test.gaztranzit.eu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2920 |
| [252838901](https://crt.sh/?id=252838901&opt=cablint) | 2016-06-03 | 2018-06-03 | C=HU, L=Budapest, O=Budapest Bank Zrt., CN=acfc.budapestbank.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2902 |
| [286778581](https://crt.sh/?id=286778581&opt=cablint) | 2016-05-25 | 2018-05-25 | C=HU, L=Budapest, O=Szellemi Tulajdon Nemzeti Hivatala, CN=host235.sztnh.gov.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2874 |
| [286789246](https://crt.sh/?id=286789246&opt=cablint) | 2016-04-19 | 2018-04-19 | C=HU, L=Budapest, O=Microsec zrt., CN=proxy-test.microsigner.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.2866 |
| [286778942](https://crt.sh/?id=286778942&opt=cablint) | 2016-03-17 | 2018-03-17 | C=HU, L=Budapest, O=Országos Rendőr-főkapitányság, CN=sip.lync.police.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2750 |
| [286812491](https://crt.sh/?id=286812491&opt=cablint) | 2016-02-16 | 2018-02-15 | C=HU, L=Budapest, O=Microsec zrt., CN=mx1.microsec.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.684 |
| [286399253](https://crt.sh/?id=286399253&opt=cablint) | 2016-02-16 | 2018-02-15 | C=HU, L=Budapest, O=Microsec zrt., CN=mx2.microsec.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.684 |
| [287116497](https://crt.sh/?id=287116497&opt=cablint) | 2016-02-16 | 2018-02-15 | C=HU, L=Budapest, O=Microsec zrt., CN=mx.microsec.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.684 |
| [221671888](https://crt.sh/?id=221671888&opt=cablint) | 2015-12-28 | 2017-12-27 | C=HU, L=Budapest, O=KEKKH, OU=Üzemeltetés, CN=nek.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2736 |
| [288911682](https://crt.sh/?id=288911682&opt=cablint) | 2015-12-02 | 2017-12-01 | C=HU, L=Budapest, O=EcoSolifer Modulgyártó Kft., CN=\*.ecosolifer.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.2788 |
| [288767633](https://crt.sh/?id=288767633&opt=cablint) | 2015-11-20 | 2017-11-19 | C=HU, L=Budapest, O=MANAGEMENT PARTNERS Holding Zrt., OU=IT, CN=\*.mphzrt.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.1295 |
| [289304693](https://crt.sh/?id=289304693&opt=cablint) | 2015-11-04 | 2017-11-03 | C=HU, L=Budapest, O=Nemzeti Média- és Hírközlési Hatóság, OU=Informatikai Igazgatóság, CN=ocsp.kgyhsz.gov.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.1441 |
| [289322356](https://crt.sh/?id=289322356&opt=cablint) | 2015-11-03 | 2017-11-02 | C=HU, L=Tiszaújváros, O=MOL Petrolkémia Zrt., CN=quickr.tvk.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2532 |
| [288736058](https://crt.sh/?id=288736058&opt=cablint) | 2015-11-03 | 2017-11-02 | C=HU, L=Tiszaújváros, O=MOL Petrolkémia Zrt., CN=sales01.tvk.eu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2325 |
| [288890128](https://crt.sh/?id=288890128&opt=cablint) | 2015-11-03 | 2017-11-02 | C=HU, L=Tiszaújváros, O=MOL Petrolkémia Zrt., CN=travdom.tvk.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2324 |
| [289985116](https://crt.sh/?id=289985116&opt=cablint) | 2015-10-28 | 2017-10-27 | C=HU, L=Budapest, O=tbsinconsult Kft., CN=ticketing.tbsinconsult.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2773 |
| [288911671](https://crt.sh/?id=288911671&opt=cablint) | 2015-10-21 | 2017-10-20 | C=HU, L=Paks, O=MVMI ZRt., OU=Infrastruktúra Üzemeltetési Osztály, CN=lyncdiscover.mvm-informatika.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.1702 |
| [288193902](https://crt.sh/?id=288193902&opt=cablint) | 2015-10-13 | 2017-10-12 | C=HU, L=Budapest, O=HAYER Kft., CN=mail.jss.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2758 |
| [288815197](https://crt.sh/?id=288815197&opt=cablint) | 2015-10-08 | 2017-10-07 | C=HU, L=Budapest, O=Budapest Bank Zrt., CN=sfbweb01.budapestbank.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2723 |
| [288783144](https://crt.sh/?id=288783144&opt=cablint) | 2015-10-02 | 2017-10-01 | C=HU, L=Pomáz, O=BATZ HUNGARY KFT., CN=mail.batz.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2742 |
| [288878237](https://crt.sh/?id=288878237&opt=cablint) | 2015-10-01 | 2017-09-30 | C=HU, L=Budapest, O=Budapest Bank Zrt., CN=mxenapp.budapestbank.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2747 |
| [289988923](https://crt.sh/?id=289988923&opt=cablint) | 2015-09-30 | 2017-09-29 | C=HU, L=Budapest, O=Fővárosi Csatornázási Művek Zrt., OU=Információs Rendszerek Osztálya, OU=Számítástechnikai Csoport, CN=mail.fcsm.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2323 |
| [289201279](https://crt.sh/?id=289201279&opt=cablint) | 2015-08-25 | 2017-08-24 | C=HU, L=Budapest, O=NEG Zrt., CN=\*.negzrt.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2714 |
| [285105409](https://crt.sh/?id=285105409&opt=cablint) | 2015-08-17 | 2017-08-16 | C=HU, L=Gyermely, O=Gyermelyi Zrt., OU=Informatika, CN=box.gyermelyi.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2713 |
| [289323346](https://crt.sh/?id=289323346&opt=cablint) | 2015-07-28 | 2017-07-27 | C=HU, L=Budapest, O=Klebelsberg Intézményfenntartó Központ, CN=\*.iskola.gov.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2702 |
| [288701782](https://crt.sh/?id=288701782&opt=cablint) | 2015-07-06 | 2017-07-05 | C=HU, L=Budapest, O=NISZ Zrt., CN=www.teszt.eleveltar.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.1836 |
| [288648030](https://crt.sh/?id=288648030&opt=cablint) | 2015-06-15 | 2017-06-14 | C=HU, L=Budapest, CN=\*.mnkhzrt.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2660 |
| [288640950](https://crt.sh/?id=288640950&opt=cablint) | 2015-04-22 | 2017-04-21 | C=HU, L=Budapest, O=NISZ Zrt., CN=szir.kef.gov.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.1766 |
| [287947822](https://crt.sh/?id=287947822&opt=cablint) | 2015-04-22 | 2017-04-21 | C=HU, L=Budapest, O=NISZ Zrt., CN=terminal.gov.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.1763 |
| [288878424](https://crt.sh/?id=288878424&opt=cablint) | 2015-02-26 | 2017-02-25 | C=HU, L=Budapest, O=Microsec Ltd., CN=scep.passbyme.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.1680 |
| [285744883](https://crt.sh/?id=285744883&opt=cablint) | 2015-02-25 | 2017-02-24 | C=HU, L=Budapest, O=Microsec Ltd., CN=m1.passbyme.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.2586 |
| [289348686](https://crt.sh/?id=289348686&opt=cablint) | 2015-01-19 | 2017-01-18 | C=HU, L=Budapest, O=Microsec Ltd., CN=mqtt-test.passbyme.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.2583 |
| [289304781](https://crt.sh/?id=289304781&opt=cablint) | 2015-01-13 | 2017-01-12 | C=HU, L=Budapest, O=ABT Hungária Tanácsadó Korlátolt Felelősségű Társaság, CN=portal.abt.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.1541 |

It was a problem in 2017. It was solved that time, all the misissued certificates were revoked and replaced as agreed by Mozilla before the end of November 2017. Since the end of November 2017 there is no valid TLS certificates with this faulty key usage.

**ERROR: Unallowed key usage for RSA public key  for 29 certificates**

|  |  |  |  |
| --- | --- | --- | --- |
| **crt.sh ID** | **Not Before** | **Not After** | **Subject Name** |
| [31806165](https://crt.sh/?id=31806165&opt=cablint) | 2016-09-05 | 2018-09-05 | C=HU, L=Budapest, O=CEEGEX Zrt., 2.5.4.97=VATHU-23408612-2-41, CN=otc.ceegex.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2491 |
| [29239747](https://crt.sh/?id=29239747&opt=cablint) | 2016-08-18 | 2018-08-18 | C=HU, L=Budapest, O=HAYER Kft., 2.5.4.97=VATHU-10778805-2-42, CN=\*.jss.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2953 |
| [24802649](https://crt.sh/?id=24802649&opt=cablint) | 2016-07-12 | 2018-07-12 | C=HU, L=Budapest, O=EUROTAX GLASS'S MAGYARORSZÁG Kft., 2.5.4.97=VATHU-10484225-2-42, CN=\*.eurotaxglass.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.1060 |
| [24292673](https://crt.sh/?id=24292673&opt=cablint) | 2016-07-07 | 2018-07-07 | C=HU, L=Budapest, O=Magyar Országos Közjegyzői Kamara, 2.5.4.97=VATHU-18000098-1-41, CN=mokk.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2929 |
| [24172696](https://crt.sh/?id=24172696&opt=cablint) | 2016-07-06 | 2018-07-06 | C=HU, L=Budapest, O=FOOLY Stúdió Kft., 2.5.4.97=VATHU-13438955-2-43, CN=www.avg.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2925 |
| [24059220](https://crt.sh/?id=24059220&opt=cablint) | 2016-07-05 | 2018-07-05 | C=HU, L=Budapest, O=Microsec Ltd., CN=\*.e-szigno.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.684 |
| [23388549](https://crt.sh/?id=23388549&opt=cablint) | 2016-06-27 | 2018-06-27 | C=HU, L=Budapest, O=NOVO PARTS TRADE Kft., CN=iroda.novoparts.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.1339 |
| [21807244](https://crt.sh/?id=21807244&opt=cablint) | 2016-06-07 | 2018-06-07 | C=HU, L=Budapest, O=Magyar Országos Közjegyzői Kamara, CN=kozjegyzok.mokk.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2907 |
| [19460254](https://crt.sh/?id=19460254&opt=cablint) | 2016-05-12 | 2018-05-12 | C=HU, L=Budapest, O=Oktatási Hivatal, CN=\*.oktatas.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2878 |
| [19505970](https://crt.sh/?id=19505970&opt=cablint) | 2016-05-12 | 2018-05-12 | C=HU, L=Budapest, O=Oktatási Hivatal, CN=www.tehetsegkapu.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2879 |
| [16881533](https://crt.sh/?id=16881533&opt=cablint) | 2016-04-15 | 2018-04-15 | C=HU, L=Budapest, O=Advisesoft Zrt., CN=support.advisesoft.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.2852 |
| [17361540](https://crt.sh/?id=17361540&opt=cablint) | 2016-04-14 | 2018-04-14 | C=HU, L=Budapest, O=CEOX Informatika Kft., CN=\*.ceoxcrm.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.2860 |
| [17076319](https://crt.sh/?id=17076319&opt=cablint) | 2016-04-12 | 2018-04-12 | C=HU, L=Budapest, O=VECTRUM Kft., CN=teleszamla.vectrum.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.750 |
| [16145440](https://crt.sh/?id=16145440&opt=cablint) | 2016-03-29 | 2018-03-29 | C=HU, L=Gyermely, O=Gyermelyi Zrt., OU=IT, CN=mail.gyermelyi.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2844 |
| [15841981](https://crt.sh/?id=15841981&opt=cablint) | 2016-03-25 | 2018-03-25 | C=HU, L=Budapest, O=Microsec Ltd., CN=sslcheck.e-szigno.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2763 |
| [15642758](https://crt.sh/?id=15642758&opt=cablint) | 2016-03-21 | 2018-03-21 | C=HU, L=Budapest, O=Microsec Ltd., CN=www.passbyme.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.1680 |
| [16725349](https://crt.sh/?id=16725349&opt=cablint) | 2016-03-21 | 2018-03-21 | C=HU, L=Budapest, O=Microsec Ltd., CN=proxy.microsigner.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.2848 |
| [15696743](https://crt.sh/?id=15696743&opt=cablint) | 2016-03-11 | 2018-03-11 | C=HU, L=Budapest, O=DLM Consulting Kft., CN=\*.dlmc.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2842 |
| [16176922](https://crt.sh/?id=16176922&opt=cablint) | 2016-03-03 | 2018-03-03 | C=HU, L=Budapest, CN=papirbol.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2837 |
| [17175621](https://crt.sh/?id=17175621&opt=cablint) | 2016-02-29 | 2018-02-28 | C=HU, L=Budapest, O=Oktatási Hivatal, CN=\*.oh.gov.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2835 |
| [13493379](https://crt.sh/?id=13493379&opt=cablint) | 2016-02-26 | 2018-02-25 | C=HU, L=Budapest, O=Sensus Informatika Kft., CN=sensus.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.1414 |
| [13651767](https://crt.sh/?id=13651767&opt=cablint) | 2016-02-16 | 2018-02-15 | C=HU, L=Budapest, O=KRIO Intézet Zrt., CN=\*.krio.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2828 |
| [12924182](https://crt.sh/?id=12924182&opt=cablint) | 2016-01-29 | 2018-01-28 | C=HU, L=Budapest, O=TR Consult Kft., CN=\*.trconsult.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2813 |
| [12037026](https://crt.sh/?id=12037026&opt=cablint) | 2016-01-12 | 2018-01-11 | C=HU, L=Budapest, O=NetworKing Informatika Kft., CN=\*.helpme.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2804 |
| [12257754](https://crt.sh/?id=12257754&opt=cablint) | 2016-01-11 | 2018-01-10 | C=HU, L=Budapest, O=NISZ Zrt., CN=\*.ugyfelkapu.gov.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2803 |
| [72959658](https://crt.sh/?id=72959658&opt=cablint) | 2015-11-18 | 2017-11-17 | C=HU, L=Budapest, O=Multi Alarm ZRT., CN=ugyfelkapu.multialarm.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.1816 |
| [89297177](https://crt.sh/?id=89297177&opt=cablint) | 2015-11-09 | 2017-11-08 | C=HU, L=Budapest, O=Alkotmányvédelmi Hivatal, OU=Informatikai és Létesítménygazdálkodási Főosztály, OU=Gazdasági és Informatikai Igazgatóság, CN=nbell.ah.gov.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2748 |
| [90149547](https://crt.sh/?id=90149547&opt=cablint) | 2015-11-09 | 2017-11-08 | C=HU, L=Budapest, O=Alkotmányvédelmi Hivatal, OU=Informatikai és Létesítménygazdálkodási Főosztály, OU=Gazdasági és Informatikai Igazgatóság, CN=bim.ah.gov.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2749 |
| [76037421](https://crt.sh/?id=76037421&opt=cablint) | 2015-05-06 | 2017-05-05 | C=HU, L=Budapest, O=OTP Faktoring Zrt., CN=\*.otpfakt.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.1733 |

It was the same problem as described above.

**ERROR: commonNames in BR certificates must be from SAN entries  in 9 certificates**

|  |  |  |  |
| --- | --- | --- | --- |
| [15642758](https://crt.sh/?id=15642758&opt=cablint) | 2016-03-21 | 2018-03-21 | C=HU, L=Budapest, O=Microsec Ltd., CN=www.passbyme.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.1680 |
| [16145440](https://crt.sh/?id=16145440&opt=cablint) | 2016-03-29 | 2018-03-29 | C=HU, L=Gyermely, O=Gyermelyi Zrt., OU=IT, CN=mail.gyermelyi.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2844 |
| [16176922](https://crt.sh/?id=16176922&opt=cablint) | 2016-03-03 | 2018-03-03 | C=HU, L=Budapest, CN=papirbol.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2837 |
| [17175621](https://crt.sh/?id=17175621&opt=cablint) | 2016-02-29 | 2018-02-28 | C=HU, L=Budapest, O=Oktatási Hivatal, CN=\*.oh.gov.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2835 |
| [31806165](https://crt.sh/?id=31806165&opt=cablint) | 2016-09-05 | 2018-09-05 | C=HU, L=Budapest, O=CEEGEX Zrt., 2.5.4.97=VATHU-23408612-2-41, CN=otc.ceegex.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2491 |
| [69175558](https://crt.sh/?id=69175558&opt=cablint) | 2016-12-16 | 2018-12-16 | C=HU, L=Budapest, O=O.F.SZ. Zrt., CN=VATHU-24134291-1-43, CN=www.fk.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2374 |
| [285105409](https://crt.sh/?id=285105409&opt=cablint) | 2015-08-17 | 2017-08-16 | C=HU, L=Gyermely, O=Gyermelyi Zrt., OU=Informatika, CN=box.gyermelyi.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2713 |
| [285744883](https://crt.sh/?id=285744883&opt=cablint) | 2015-02-25 | 2017-02-24 | C=HU, L=Budapest, O=Microsec Ltd., CN=m1.passbyme.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.2586 |
| [608762420](https://crt.sh/?id=608762420&opt=cablint) | 2018-07-24 | 2021-07-24 | C=HU, L=Budapest, O=Microsec zrt., CN=MICRODC2.ad.iroda.microsec.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.684 |

6 of these certificates were issued without SAN, see next section.

The other certificates are:

<https://crt.sh/?id=608762420&opt=cablint>

This domain controller certificate was issued on 2018-07-24.

It had several problems which were recognized during the post issuance certificate test, so the certificate has not been published and used. It was revoked on 2018-07-25.

It contained a typing mistake in the commonName.

It has not been issued according to the BR because it is not a TLS certificate.

This issue was discussed earlier with Mozilla

(see in <https://groups.google.com/forum/#!topic/mozilla.dev.security.policy/Pcc1_luzwNs> and <https://bugzilla.mozilla.org/show_bug.cgi?id=1512270> ), so in the future Microsec will issue also domain controller and CISCO VPN certificates according to the BR.

<https://crt.sh/?id=69175558&opt=cablint>

This certificate contains two commonName fields, one of them contains the VAT number of the company which should be in the organization Identifier field.

It was the result of a human mistake during the issuance.

The certificate was revoked on 2017-08-16.

When this fault was recognized we developed and introduced further automatic checks in the CA program to avoid issuing certificates with this fault.

<https://crt.sh/?id=15642758&opt=cablint>

**ERROR: commonNames in BR certificates must be from SAN entries**

The certificate contains [www.passbyme.com](http://www.passbyme.com) in the commonName and \*.passbyme.com in the SAN which is logically correct but they are not the same entries byte by byte.

The certificate was revoked on 2017-01-05.

New automatism was introduced in the CA program to check the fulfilment of this requirement.

**ERROR: commonNames in BR certificates must be from SAN entries  in 6 certificates**

|  |  |  |  |
| --- | --- | --- | --- |
| [16145440](https://crt.sh/?id=16145440&opt=cablint) | 2016-03-29 | 2018-03-29 | C=HU, L=Gyermely, O=Gyermelyi Zrt., OU=IT, CN=mail.gyermelyi.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2844 |
| [16176922](https://crt.sh/?id=16176922&opt=cablint) | 2016-03-03 | 2018-03-03 | C=HU, L=Budapest, CN=papirbol.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2837 |
| [17175621](https://crt.sh/?id=17175621&opt=cablint) | 2016-02-29 | 2018-02-28 | C=HU, L=Budapest, O=Oktatási Hivatal, CN=\*.oh.gov.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2835 |
| [31806165](https://crt.sh/?id=31806165&opt=cablint) | 2016-09-05 | 2018-09-05 | C=HU, L=Budapest, O=CEEGEX Zrt., 2.5.4.97=VATHU-23408612-2-41, CN=otc.ceegex.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2491 |
| [285105409](https://crt.sh/?id=285105409&opt=cablint) | 2015-08-17 | 2017-08-16 | C=HU, L=Gyermely, O=Gyermelyi Zrt., OU=Informatika, CN=box.gyermelyi.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2713 |
| [285744883](https://crt.sh/?id=285744883&opt=cablint) | 2015-02-25 | 2017-02-24 | C=HU, L=Budapest, O=Microsec Ltd., CN=m1.passbyme.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.2586 |

These old certificates were issued without SAN entry.

They were removed more than 2 years ago on the 2017-01-05.

**ERROR: BR certificates without organizationName must not include localityName  in 2 certificates**

|  |  |  |  |
| --- | --- | --- | --- |
| **crt.sh ID** | **Not Before** | **Not After** | **Subject Name** |
| [16176922](https://crt.sh/?id=16176922&opt=cablint) | 2016-03-03 | 2018-03-03 | C=HU, L=Budapest, CN=papirbol.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2837 |
| [288648030](https://crt.sh/?id=288648030&opt=cablint) | 2015-06-15 | 2017-06-14 | C=HU, L=Budapest, CN=\*.mnkhzrt.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2660 |

<https://crt.sh/?id=16176922&opt=cablint>

This certificate was issued on 2016-03-03 with two years validity according to the ETSI NCP policy (0.4.0.2042.1.1).

The certificate doesn’t have SAN field.

After recognizing the fault the certificate was revoked on 2017-01-05 as part of a bigger revision process.

The presently issued certificates already contains the localityName only in case of IVCP or OVCP certificate, it is not filled in case of DVCP certificate.

<https://crt.sh/?id=288648030&opt=cablint>

This certificate was issued on 2015-07-15 with two years validity according to the ETSI NCP policy (0.4.0.2042.1.1) and it expired on 2017-06-14.

The expiry of the certificate was earlier than the deadline for revoking the misissued certificates with the Key Agreement problem so it has not been revoked.

The presently issued TLS certificates contain the localityName only in case of IVCP or OVCP certificate, it is not filled in case of DVCP certificate.

**ERROR: BR certificates must be 825 days in validity or less  in 1 certificate**

<https://crt.sh/?cablint=1104&iCAID=1536&minNotBefore=2015-01-01>

This was a misissued domain controller certificate, the case has already been answered.

**ERROR: DNSName is not FQDN**

**and**

**ERROR: Constraint failure in SubjectAltName: ASN.1 constraint check failed: IA5String: value byte 2 out of range: 195 > 127 (IA5String.c:64)**

**in 1 certificate**

<https://crt.sh/?cablint=93&iCAID=1536&minNotBefore=2015-01-01>

The certificate was issued to the Hungarian Chamber of Notaries on 2017-05-26 for two years. It contains several DNSName entries in the SAN, some of them contains special Hungarian characters, like ‘ö’.

The fault was caused by the unproper coding of these DNSName entries.

After recognising the fault the certificate was revoked on 2017-08-10.

To avoid having the same problem again we included further checks on the content of the DNSName entries in the CA program.

**ERROR: BR certificates must not contain otherName type alternative name  in 1 certificate**

<https://crt.sh/?cablint=210&iCAID=1536&minNotBefore=2015-01-01>

This domain controller certificate has already been answered.

**X.509 lint**

**ERROR: Invalid type in SAN entry  in 31 certificates**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |
| --- | --- | --- | --- |
| **crt.sh ID** | **Not Before** | **Not After** | **Subject Name** |
| [608762420](https://crt.sh/?id=608762420&opt=x509lint) | 2018-07-24 | 2021-07-24 | C=HU, L=Budapest, O=Microsec zrt., CN=MICRODC2.ad.iroda.microsec.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.684 |
| [392942949](https://crt.sh/?id=392942949&opt=x509lint) | 2018-04-12 | 2018-04-13 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [318275046](https://crt.sh/?id=318275046&opt=x509lint) | 2018-02-01 | 2018-02-02 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [284018050](https://crt.sh/?id=284018050&opt=x509lint) | 2017-12-21 | 2017-12-22 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [270580322](https://crt.sh/?id=270580322&opt=x509lint) | 2017-12-04 | 2017-12-05 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [250661716](https://crt.sh/?id=250661716&opt=x509lint) | 2017-11-09 | 2017-11-10 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [245331623](https://crt.sh/?id=245331623&opt=x509lint) | 2017-11-01 | 2017-11-02 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [220563988](https://crt.sh/?id=220563988&opt=x509lint) | 2017-09-30 | 2017-10-01 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [214027024](https://crt.sh/?id=214027024&opt=x509lint) | 2017-09-20 | 2017-09-21 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [201186490](https://crt.sh/?id=201186490&opt=x509lint) | 2017-08-29 | 2017-08-30 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [201260319](https://crt.sh/?id=201260319&opt=x509lint) | 2017-08-28 | 2017-08-29 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [198369537](https://crt.sh/?id=198369537&opt=x509lint) | 2017-08-25 | 2017-08-26 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [191642501](https://crt.sh/?id=191642501&opt=x509lint) | 2017-08-16 | 2017-08-17 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [175334356](https://crt.sh/?id=175334356&opt=x509lint) | 2017-07-19 | 2017-07-20 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [167223163](https://crt.sh/?id=167223163&opt=x509lint) | 2017-07-05 | 2017-07-06 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [160110916](https://crt.sh/?id=160110916&opt=x509lint) | 2017-06-23 | 2017-06-24 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [154664764](https://crt.sh/?id=154664764&opt=x509lint) | 2017-06-15 | 2017-06-16 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [143128673](https://crt.sh/?id=143128673&opt=x509lint) | 2017-05-23 | 2017-05-24 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [139648909](https://crt.sh/?id=139648909&opt=x509lint) | 2017-05-17 | 2017-05-18 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [137045443](https://crt.sh/?id=137045443&opt=x509lint) | 2017-05-12 | 2017-05-13 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136466700](https://crt.sh/?id=136466700&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136429482](https://crt.sh/?id=136429482&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136388978](https://crt.sh/?id=136388978&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136243496](https://crt.sh/?id=136243496&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136243459](https://crt.sh/?id=136243459&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136242596](https://crt.sh/?id=136242596&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136242577](https://crt.sh/?id=136242577&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136220429](https://crt.sh/?id=136220429&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136184653](https://crt.sh/?id=136184653&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [135966897](https://crt.sh/?id=135966897&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [158776082](https://crt.sh/?id=158776082&opt=x509lint) | 2015-12-15 | 2017-12-14 | C=HU, L=Budapest, O=Microsec Ltd., CN=Microsec, emailAddress=info@e-szigno.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.22 |

 |

The list contains 29 OCSP responder certificates, which contain the email entry in the SAN.

[608762420](https://crt.sh/?id=608762420) CN=MICRODC2.ad.iroda.microsec.hu was a really misissued certificate, it has been already answered.

[158776082](https://crt.sh/?id=158776082)

is a code signing certificate, it contains the email entry in the SAN.

**ERROR: No OCSP over HTTP  in 29 certificates**

|  |  |  |  |
| --- | --- | --- | --- |
| **crt.sh ID** | **Not Before** | **Not After** | **Subject Name** |
| [392942949](https://crt.sh/?id=392942949&opt=x509lint) | 2018-04-12 | 2018-04-13 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [318275046](https://crt.sh/?id=318275046&opt=x509lint) | 2018-02-01 | 2018-02-02 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [284018050](https://crt.sh/?id=284018050&opt=x509lint) | 2017-12-21 | 2017-12-22 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [270580322](https://crt.sh/?id=270580322&opt=x509lint) | 2017-12-04 | 2017-12-05 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [250661716](https://crt.sh/?id=250661716&opt=x509lint) | 2017-11-09 | 2017-11-10 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [245331623](https://crt.sh/?id=245331623&opt=x509lint) | 2017-11-01 | 2017-11-02 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [220563988](https://crt.sh/?id=220563988&opt=x509lint) | 2017-09-30 | 2017-10-01 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [214027024](https://crt.sh/?id=214027024&opt=x509lint) | 2017-09-20 | 2017-09-21 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [201186490](https://crt.sh/?id=201186490&opt=x509lint) | 2017-08-29 | 2017-08-30 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [201260319](https://crt.sh/?id=201260319&opt=x509lint) | 2017-08-28 | 2017-08-29 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [198369537](https://crt.sh/?id=198369537&opt=x509lint) | 2017-08-25 | 2017-08-26 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [191642501](https://crt.sh/?id=191642501&opt=x509lint) | 2017-08-16 | 2017-08-17 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [175334356](https://crt.sh/?id=175334356&opt=x509lint) | 2017-07-19 | 2017-07-20 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [167223163](https://crt.sh/?id=167223163&opt=x509lint) | 2017-07-05 | 2017-07-06 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [160110916](https://crt.sh/?id=160110916&opt=x509lint) | 2017-06-23 | 2017-06-24 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [154664764](https://crt.sh/?id=154664764&opt=x509lint) | 2017-06-15 | 2017-06-16 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [143128673](https://crt.sh/?id=143128673&opt=x509lint) | 2017-05-23 | 2017-05-24 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [139648909](https://crt.sh/?id=139648909&opt=x509lint) | 2017-05-17 | 2017-05-18 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [137045443](https://crt.sh/?id=137045443&opt=x509lint) | 2017-05-12 | 2017-05-13 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136466700](https://crt.sh/?id=136466700&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136429482](https://crt.sh/?id=136429482&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136388978](https://crt.sh/?id=136388978&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136243496](https://crt.sh/?id=136243496&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136243459](https://crt.sh/?id=136243459&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136242596](https://crt.sh/?id=136242596&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136242577](https://crt.sh/?id=136242577&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136220429](https://crt.sh/?id=136220429&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [136184653](https://crt.sh/?id=136184653&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |
| [135966897](https://crt.sh/?id=135966897&opt=x509lint) | 2017-05-11 | 2017-05-12 | C=HU, L=Budapest, O=Microsec Ltd., CN=e-Szigno SSL CA 2014 OCSP Responder, emailAddress=info@e-szigno.hu |

All these certificates are OCSP responder certificates, there is no revocation for these short life certificates at all. This case has already been answered.

**ERROR: No Subject alternative name extension  in 18 certificates**

|  |  |  |  |
| --- | --- | --- | --- |
| **crt.sh ID** | **Not Before** | **Not After** | **Subject Name** |
| [31806165](https://crt.sh/?id=31806165&opt=x509lint) | 2016-09-05 | 2018-09-05 | C=HU, L=Budapest, O=CEEGEX Zrt., 2.5.4.97=VATHU-23408612-2-41, CN=otc.ceegex.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2491 |
| [42379651](https://crt.sh/?id=42379651&opt=x509lint) | 2016-07-28 | 2018-07-28 | C=HU, L=Kecskemét, O=Silveria Kft., 2.5.4.97=VATHU-12807574-2-03, CN=mail.silveria.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2487 |
| [26286155](https://crt.sh/?id=26286155&opt=x509lint) | 2016-07-18 | 2018-07-18 | C=HU, L=Budapest, CN=pointnet.pointmedia.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2468 |
| [23465795](https://crt.sh/?id=23465795&opt=x509lint) | 2016-05-31 | 2018-05-31 | C=HU, L=Budapest, O=Budapest Bank Zrt., CN=extsso.budapestbank.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2901 |
| [158871338](https://crt.sh/?id=158871338&opt=x509lint) | 2016-04-07 | 2018-04-07 | C=HU, L=Keszthely, CN=Baloghy Szoftver Kft., serialNumber=1.3.6.1.4.1.21528.2.3.2.2321 |
| [16145440](https://crt.sh/?id=16145440&opt=x509lint) | 2016-03-29 | 2018-03-29 | C=HU, L=Gyermely, O=Gyermelyi Zrt., OU=IT, CN=mail.gyermelyi.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2844 |
| [16176922](https://crt.sh/?id=16176922&opt=x509lint) | 2016-03-03 | 2018-03-03 | C=HU, L=Budapest, CN=papirbol.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2837 |
| [17175621](https://crt.sh/?id=17175621&opt=x509lint) | 2016-02-29 | 2018-02-28 | C=HU, L=Budapest, O=Oktatási Hivatal, CN=\*.oh.gov.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2835 |
| [158780955](https://crt.sh/?id=158780955&opt=x509lint) | 2016-02-18 | 2018-02-17 | C=HU, L=Gyöngyös, CN=WSOFT.HU - Fehér Attila, serialNumber=1.3.6.1.4.1.21528.2.3.2.1380 |
| [158878709](https://crt.sh/?id=158878709&opt=x509lint) | 2016-02-05 | 2018-02-04 | C=HU, L=Budapest, O=NOVITAX KFT., CN=Novitax Kft., serialNumber=1.3.6.1.4.1.21528.2.3.2.1395 |
| [158881101](https://crt.sh/?id=158881101&opt=x509lint) | 2016-01-18 | 2018-01-17 | C=HU, L=Budapest, O=eGOV Kft., OU=Development, CN=Egov - Cégírnok, serialNumber=1.3.6.1.4.1.21528.2.3.2.1316 |
| [158851911](https://crt.sh/?id=158851911&opt=x509lint) | 2015-12-04 | 2017-12-03 | C=HU, L=Baja, O=FORINT-Soft Kft., CN=FORINT-Soft Kft., serialNumber=1.3.6.1.4.1.21528.2.3.2.2794 |
| [158777331](https://crt.sh/?id=158777331&opt=x509lint) | 2015-11-12 | 2017-11-11 | C=HU, L=Zalaegerszeg, O=NEEDIT SERVICES Kft., CN=needIT Services Kft., serialNumber=1.3.6.1.4.1.21528.2.3.2.2779 |
| [158868263](https://crt.sh/?id=158868263&opt=x509lint) | 2015-10-16 | 2017-10-15 | C=HU, L=Budapest, O=Budapesti Értéktőzsde Zrt., CN=Budapesti Értéktőzsde Zrt., serialNumber=1.3.6.1.4.1.21528.2.3.2.115 |
| [285105409](https://crt.sh/?id=285105409&opt=x509lint) | 2015-08-17 | 2017-08-16 | C=HU, L=Gyermely, O=Gyermelyi Zrt., OU=Informatika, CN=box.gyermelyi.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2713 |
| [158782429](https://crt.sh/?id=158782429&opt=x509lint) | 2015-08-12 | 2017-08-11 | C=HU, L=Budapest, O=UNIX AUTÓ KFT., CN=Unix Autó Kft., serialNumber=1.3.6.1.4.1.21528.2.3.2.2711 |
| [158870202](https://crt.sh/?id=158870202&opt=x509lint) | 2015-08-05 | 2017-08-04 | C=HU, L=Szombathely, O=DATAFLEX HUNGARY KFT., OU=InnVoice Ügyfélszolgálat, CN=Dataflex Hungary Kft., serialNumber=1.3.6.1.4.1.21528.2.3.2.1483 |
| [285744883](https://crt.sh/?id=285744883&opt=x509lint) | 2015-02-25 | 2017-02-24 | C=HU, L=Budapest, O=Microsec Ltd., CN=m1.passbyme.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.2586 |

These certificates were issued between 2015-02-02 and 2016-09-05 for two years and they really do not have SAN entry.

There are several faulty SSL certificate amoung them, but there are other type of certificates too.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **crt.sh ID** | **Not Before** | **Not After** | **Subject Name** | **comment** |
| [31806165](https://crt.sh/?id=31806165&opt=x509lint) | 2016-09-05 | 2018-09-05 | CN=otc.ceegex.hu | revoked on 2017-01-05 |
| [42379651](https://crt.sh/?id=42379651&opt=x509lint) | 2016-07-28 | 2018-07-28 | CN=mail.silveria.hu | revoked on 2017-01-05 |
| [26286155](https://crt.sh/?id=26286155&opt=x509lint) | 2016-07-18 | 2018-07-18 | CN=pointnet.pointmedia.hu | revoked on 2017-01-05 |
| [23465795](https://crt.sh/?id=23465795&opt=x509lint) | 2016-05-31 | 2018-05-31 | CN=extsso.budapestbank.hu | revoked on 2017-01-05 |
| [158871338](https://crt.sh/?id=158871338&opt=x509lint) | 2016-04-07 | 2018-04-07 | CN=Baloghy Szoftver Kft. | code signing |
| [16145440](https://crt.sh/?id=16145440&opt=x509lint) | 2016-03-29 | 2018-03-29 | CN=mail.gyermelyi.hu | revoked on 2017-01-05 |
| [16176922](https://crt.sh/?id=16176922&opt=x509lint) | 2016-03-03 | 2018-03-03 | CN=papirbol.hu | revoked on 2017-01-05 |
| [17175621](https://crt.sh/?id=17175621&opt=x509lint) | 2016-02-29 | 2018-02-28 | CN=\*.oh.gov.hu | revoked on 2017-01-05 |
| [158780955](https://crt.sh/?id=158780955&opt=x509lint) | 2016-02-18 | 2018-02-17 | CN=WSOFT.HU - Fehér Attila | code signing |
| [158878709](https://crt.sh/?id=158878709&opt=x509lint) | 2016-02-05 | 2018-02-04 | CN=Novitax Kft. | code signing |
| [158881101](https://crt.sh/?id=158881101&opt=x509lint) | 2016-01-18 | 2018-01-17 | CN=Egov – Cégírnok | code signing |
| [158851911](https://crt.sh/?id=158851911&opt=x509lint) | 2015-12-04 | 2017-12-03 | CN=FORINT-Soft Kft. | code signing |
| [158777331](https://crt.sh/?id=158777331&opt=x509lint) | 2015-11-12 | 2017-11-11 | CN=needIT Services Kft. | code signing |
| [158868263](https://crt.sh/?id=158868263&opt=x509lint) | 2015-10-16 | 2017-10-15 | CN=Budapesti Értéktőzsde Zrt. | code signing |
| [285105409](https://crt.sh/?id=285105409&opt=x509lint) | 2015-08-17 | 2017-08-16 | CN=box.gyermelyi.hu | revoked on 2017-01-02 |
| [158782429](https://crt.sh/?id=158782429&opt=x509lint) | 2015-08-12 | 2017-08-11 | CN=Unix Autó Kft. | code signing |
| [158870202](https://crt.sh/?id=158870202&opt=x509lint) | 2015-08-05 | 2017-08-04 | CN=Dataflex Hungary Kft. | code signing |
| [285744883](https://crt.sh/?id=285744883&opt=x509lint) | 2015-02-25 | 2017-02-24 | CN=m1.passbyme.com | revoked on 2017-01-02 |

The 9 TLS certificates were removed at latest on 2017-01-05.

The actual CA program always includes the domain names in the SAN, so there is no this problem in the new TLS certificates.

The code signing certificates do not have to contain SAN entry. These certificates are included in the error list, but this error is not indicated when I check the individual certificate.

**ERROR: Subject without organizationName, givenName or surname but with stateOrProvince or localityName  in 3 certificates**

These certificates were issued between 2015-06-15 and 2016-04-07 for two years.

|  |  |  |  |
| --- | --- | --- | --- |
| [158871338](https://crt.sh/?id=158871338&opt=x509lint) | 2016-04-07 | 2018-04-07 | C=HU, L=Keszthely, CN=Baloghy Szoftver Kft., serialNumber=1.3.6.1.4.1.21528.2.3.2.2321 |
| [158780955](https://crt.sh/?id=158780955&opt=x509lint) | 2016-02-18 | 2018-02-17 | C=HU, L=Gyöngyös, CN=WSOFT.HU - Fehér Attila, serialNumber=1.3.6.1.4.1.21528.2.3.2.1380 |
| [288648030](https://crt.sh/?id=288648030&opt=x509lint) | 2015-06-15 | 2017-06-14 | C=HU, L=Budapest, CN=\*.mnkhzrt.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2660 |

Two of them are code signing certificates.

The third certificate is an SSL certificate which is expired on 2017-06-14.

**ERROR: Subject without organizationName but with stateOrProvince or localityName  in 3 certificates**

|  |  |  |  |
| --- | --- | --- | --- |
| **crt.sh ID** | **Not Before** | **Not After** | **Subject Name** |
| [42025189](https://crt.sh/?id=42025189&opt=x509lint) | 2016-09-12 | 2018-09-12 | C=BH, L=Amwaj Islands, CN=mail.andraspeller.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.2960 |
| [26286155](https://crt.sh/?id=26286155&opt=x509lint) | 2016-07-18 | 2018-07-18 | C=HU, L=Budapest, CN=pointnet.pointmedia.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2468 |
| [16176922](https://crt.sh/?id=16176922&opt=x509lint) | 2016-03-03 | 2018-03-03 | C=HU, L=Budapest, CN=papirbol.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2837 |

These SSL certificates were issued between 2016-03-03 and 2016-09-12 with localityName without having the organizationName. for two years.

All of them were revoked in 2017.

**ERROR: Invalid user notice type  in 2 certificates**

|  |  |  |  |
| --- | --- | --- | --- |
| **crt.sh ID** | **Not Before** | **Not After** | **Subject Name** |
| [16794802](https://crt.sh/?id=16794802&opt=x509lint) | 2015-12-30 | 2017-12-29 | C=HU, L=Budapest, O=NISZ Zrt., CN=\*.niszavdh.gov.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2801 |
| [18614976](https://crt.sh/?id=18614976&opt=x509lint) | 2015-09-29 | 2017-09-28 | C=HU, L=Budapest, O=FOOLY Stúdió Kft., CN=\*.fooly.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2423 |

These certificates were issued in 2015 with explicitText coded other than UTF8String.

We changed our CA configuration in 2017 and since that the User notice is coded in UTF8.

**ZLint**

**ERROR: Explicit text has a maximum size of 200 characters  in 88 certificates**

I do not want to list all the listed certificates here.

These certificates were issued between 2015-01-13 and 2017-07-31 for two years, so a few of them is still valid.

The problem can be that the UserNotice text contains special Hungarian characters which are coded in UTF8 in more than one byte. The length of the text with 200 characters is typically longer than 200 bytes due to the UTF8 coding.

The requirement says 200 characters and not 200 bytes.

Our typical UserNotice text is 193 characters long which is coded in more than 200 bytes. The earlier version of the zlint program checked the length of the text in bytes, not in characters, so this is the reason why we had these errors.

We have recognized the problem in the zlint source and reported the problem to the authors of the program. The program was modified and a new version was issued which checks the length correctly.

See the following links:

<https://github.com/zmap/zlint/issues/242>

<https://github.com/zmap/zlint/pull/244>

**ERROR: Subscriber Certificates issued after 1 March 2018 MUST have a Validity Period no greater than 825 days.  for 6 certificates**

|  |  |  |  |
| --- | --- | --- | --- |
| **crt.sh ID** | **Not Before** | **Not After** | **Subject Name** |
| [950822028](https://crt.sh/?id=950822028&opt=zlint) | 2018-11-16 | 2021-11-16 | C=HU, L=Budapest, O=Magyar Országos Közjegyzői Kamara, CN=avpn.mokk.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.391 |
| [950784131](https://crt.sh/?id=950784131&opt=zlint) | 2018-11-16 | 2021-11-16 | C=HU, L=Budapest, O=Microsec zrt., CN=vpn1.dplx.microsec.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.684 |
| [950784016](https://crt.sh/?id=950784016&opt=zlint) | 2018-11-16 | 2021-11-16 | C=HU, L=Budapest, O=Microsec zrt., CN=vpn2.microsec.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.684 |
| [948644767](https://crt.sh/?id=948644767&opt=zlint) | 2018-11-15 | 2021-11-15 | C=HU, L=Budapest, O=Magyar Országos Közjegyzői Kamara, CN=bvpn.mokk.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.1842 |
| [946009846](https://crt.sh/?id=946009846&opt=zlint) | 2018-11-14 | 2021-11-14 | C=HU, L=Budapest, O=Magyar Országos Közjegyzői Kamara, CN=fvpn.mokk.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2565 |
| [608762420](https://crt.sh/?id=608762420&opt=zlint) | 2018-07-24 | 2021-07-24 | C=HU, L=Budapest, O=Microsec zrt., CN=MICRODC2.ad.iroda.microsec.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.684 |

These are special purpose server certificates (not TLS) and were issued for 3 years. When the problem was reported to Microsec we discussed the situation with Mozilla.

The problem is that there is no way to make clear difference between the TLS certificates and other similar certificates like CISCO VPN server or domain controller.

We revoked these certificates and replaced them with others with 2 years validity.

In the future Microsec will issue these special purpose server certificates according to the BR too.

See:

<https://groups.google.com/forum/#!topic/mozilla.dev.security.policy/Pcc1_luzwNs>

<https://bugzilla.mozilla.org/show_bug.cgi?id=1512270>

**ERROR: The common name field in subscriber certificates must include only names from the SAN extension  in 3 certificates**

|  |  |  |  |
| --- | --- | --- | --- |
| **crt.sh ID** | **Not Before** | **Not After** | **Subject Name** |
| [608762420](https://crt.sh/?id=608762420&opt=zlint) | 2018-07-24 | 2021-07-24 | C=HU, L=Budapest, O=Microsec zrt., CN=MICRODC2.ad.iroda.microsec.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.684 |
| [285105409](https://crt.sh/?id=285105409&opt=zlint) | 2015-08-17 | 2017-08-16 | C=HU, L=Gyermely, O=Gyermelyi Zrt., OU=Informatika, CN=box.gyermelyi.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2713 |
| [285744883](https://crt.sh/?id=285744883&opt=zlint) | 2015-02-25 | 2017-02-24 | C=HU, L=Budapest, O=Microsec Ltd., CN=m1.passbyme.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.2586 |

All these problems have been already answered earlier.

The ‘MICRODC2.ad.iroda.microsec.hu’ was a misissued certificate and revoked within one day after the issuance.

The two other certificates were issued in 2015 and were revoked on 2017-01-02.

**ERROR: Subscriber certificates MUST contain the Subject Alternate Name extension  in 2 certificates**

|  |  |  |  |
| --- | --- | --- | --- |
| **crt.sh ID** | **Not Before** | **Not After** | **Subject Name** |
| [285105409](https://crt.sh/?id=285105409&opt=zlint) | 2015-08-17 | 2017-08-16 | C=HU, L=Gyermely, O=Gyermelyi Zrt., OU=Informatika, CN=box.gyermelyi.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.2713 |
| [285744883](https://crt.sh/?id=285744883&opt=zlint) | 2015-02-25 | 2017-02-24 | C=HU, L=Budapest, O=Microsec Ltd., CN=m1.passbyme.com, serialNumber=1.3.6.1.4.1.21528.2.3.2.2586 |

All these problems have been already answered earlier.

The two certificates were issued in 2015 and were revoked on 2017-01-02.

**ERROR: The Subject Alternate Name extension MUST contain only 'dnsName' and 'ipaddress' name types.  in 1 certificate**

|  |  |  |  |
| --- | --- | --- | --- |
| **crt.sh ID** | **Not Before** | **Not After** | **Subject Name** |
| [608762420](https://crt.sh/?id=608762420&opt=zlint) | 2018-07-24 | 2021-07-24 | C=HU, L=Budapest, O=Microsec zrt., CN=MICRODC2.ad.iroda.microsec.hu, serialNumber=1.3.6.1.4.1.21528.2.3.2.684 |

The faulty certificate was revoked next day after the issuance.