CS-C3130 Information Security
Examination 2022-10-20
Teachers: Tuomas Aura, Lachlan Gunn

No reference materials, pocket calculators, or other auxiliary equipment are allowed in this examination.

1. Access control terminology

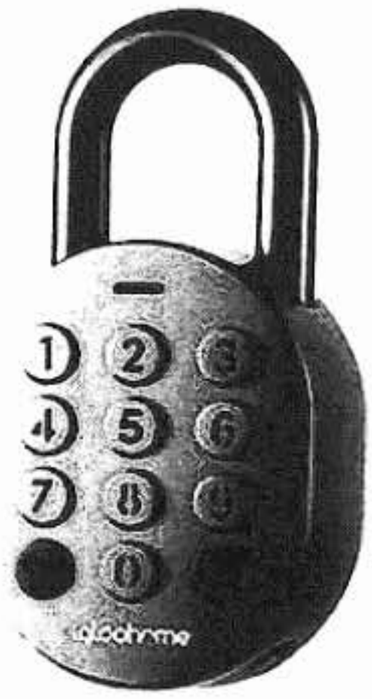
Give an example of each of the following in the context of a university or school. The example should clearly demonstrate that you have understood the meaning of the concept. The answer should be an example; no points will be given for a definition. (2p each)

1. subject and object
2. no-write-down policy
3. data sanitization

read up
write down

2. Brute-force attack

An electronic smart combination lock is opened by entering a 6-digit code with the numeric keypad and pressing the Open button. With practice, entering the code takes approximately 2 seconds. A student housing company has decided to install such locks on all the hundreds of basement storage units in the dormitory buildings. Each lock is configured with a short-distance wireless interface (Bluetooth) to have an independent random code.



Picture source: igloohome Smart Padlock

A master burglar starts a brute-force attack to find the correct combination for one storage unit. During an 8-hour workday, they can try 8*60*60/2 = 14400 combinations. Thus, their success probability of opening a lock is 14400/1000000 = 1.44 %. This worries some students who store their overalls and other valuables in the units.

The master burglar heads a gang of 100 bachelor burglars who parallelize the work by trying combinations on different locks. Their success probability of opening at least one lock during the workday is 76 %. Thus, they are very likely to succeed in breaking into some storage units over time.

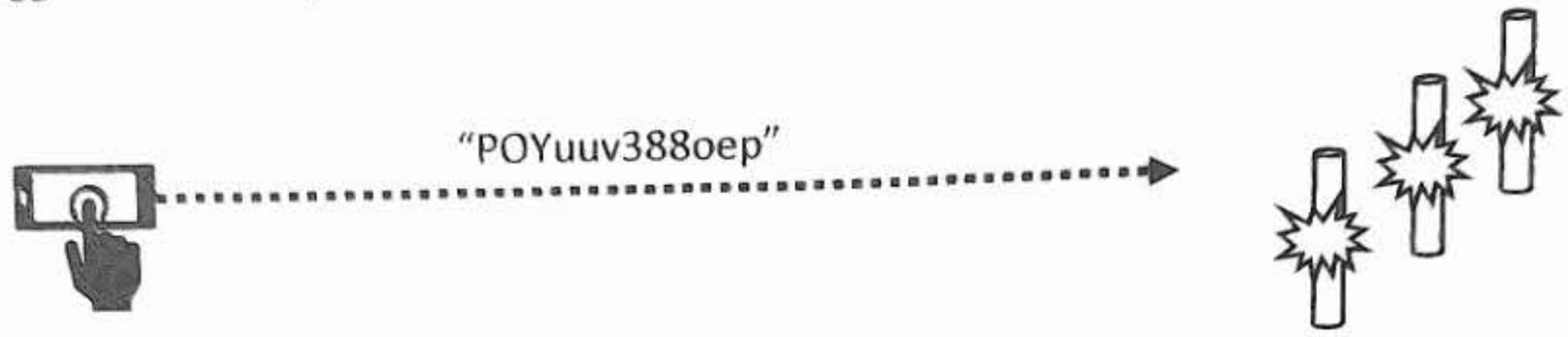
Problem: Suggest effective smart features that the locks could implement to mitigate these two types of attacks. The attacker's success probability should be smaller, but the lock hardware and user experience should be the same. (2p)

The examination continues on the following page.

3. Network security

A mineral mining company is developing a remote wireless detonator. A control panel sends a wireless trigger message to one or more smart fuses, each of which sets off an explosive. Currently, the trigger message is a one-time passphrase (for example, "192YGCiiaWPL") that is preconfigured in all the fuses used at that time. When the fuses receive this message over the wireless channel, they detonate the explosives. The company is worried about wireless hackers who could interfere with the system over the radio channel.

(a) Analyze the security of this solution against the wireless attacker. (4p)
(b) Suggest how to improve the security of the system. (2p)



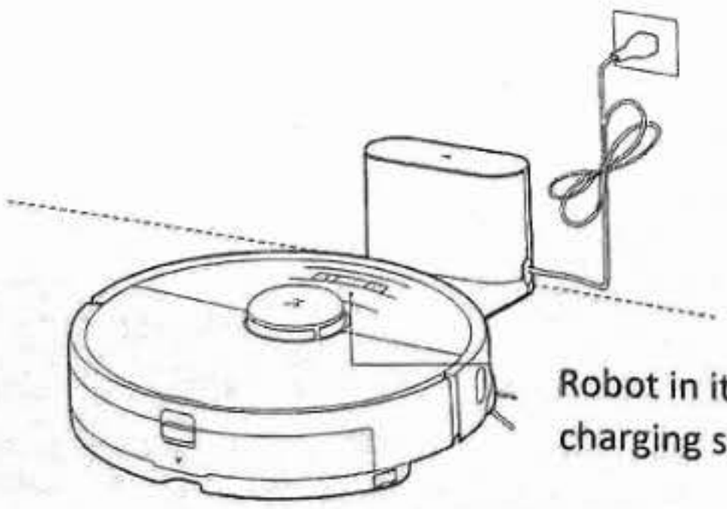
4. Threat analysis

A robotic vacuum cleaner cleans floors autonomously. It has a built-in camera for mapping the floor and for navigating around it. Computer vision also allows the robot to identify obstacles, such as furniture and pets.

The robot is connected to a cloud server over Wi-Fi wireless network. Some of the mapping and learning features have been offloaded to the cloud, while the real-time control is in the robot itself. The user interface is a mobile app, which connects to the same cloud service. (There is no direct connection between the mobile app and the robot.)

When the robot battery needs recharging, it returns to the charging station. However, all the intelligence is in the robot itself or in the cloud.

Vacuum robot with camera in the front



Robot in its charging station

Mobile app screenshot with an automatically created map

Picture sources: Roborock and user Facebook post

Problem: Analyze the security threats against the robotic vacuum cleaner system and its users. 6p

Hint: Draw a diagram of the system architecture with the data flows.

The examination continues on the following page.

5. Web security

In Appendix 1, there is a pretty-printed certificate chain. Explain in detail how the web browser checks <u>this specific</u> certificate chain and how the browser uses it to authenticate the website in TLS. (6p)

Notes: You do not need to explain the details of the TLS handshake protocol.

Appendix 1

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:ba:f8:c8:10:2b:fb:e0:e9:5a:0c:fd:10:d0:32:47:e0:c9
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Let's Encrypt, CN = R3
        Validity
            Not Before: Oct 16 22:11:41 2022 GMT
            Not After : Jan 14 22:11:40 2023 GMT
        Subject: CN = secclo.eu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:ab:58:21:01:8f:55:90:c9:81:85:0d:88:8e:f3:
                    8c:7a:4a:e3:45:ba:d9:ff:c7:23:59:5d:fa:4a:c4:
                    d6:5a:f0:86:28:8f:5d:88:dc:38:29:46:7c:e6:a3:
                    a9:3f:7e:ce:db:77:29:70:22:df:75:4c:76:eb:5e:
                    ca:ce:e4:78:3c:bf:4d:00:3c:cc:e0:19:19:2c:ea:
                    4f:39:b2:78:5e:ec:11:8b:b9:32:5e:08:8c:82:a4:
                    c8:38:71:74:a9:99:b4:e9:ab:7e:b5:46:52:e2:e9:
                    f3:52:17:54:3b:c0:91:9f:12:f5:ce:d5:f4:ce:e5:
                    a3:be:69:3e:52:a8:ac:35:48:bf:f1:2d:ac:bd:3b:
                    c3:5f:97:17:79:e9:9e:83:0c:70:4b:d7:74:e4:62:
                    cf:e2:34:7d:d9:ee:2a:02:ed:54:7b:0f:6b:8f:6f:
                    6c:43:2b:89:69:99:22:14:d8:ba:d7:ea:50:3f:3a:
                    10:5b:dc:e2:b2:eb:33:62:3d:a9:7f:e3:04:2e:7b:
                    1e:22:55:41:8e:27:5e:36:96:83:ba:43:ff:04:2f:
                    b4:c8:92:6b:e2:95:c4:76:29:24:f0:8c:a7:d8:0e:
                    be:30:2b:8c:89:84:20:9c:3a:9d:7f:e9:33:23:db:
                    9a:83:1c:84:8c:71:b0:d8:7c:cd:f6:ae:e6:14:da:
                    4a:be:33:66:2a:84:8b:0f:d5:46:2c:1d:8d:04:99:
                    cc:25:19:be:fc:d3:ce:42:f3:a4:00:52:29:a7:aa:
                    02:a4:02:fa:6b:f6:4c:0b:ed:f2:14:31:c4:33:23:
                    8e:d2:87:00:6a:c5:1c:91:53:a8:61:d7:42:f1:74:
                    3a:17:90:6c:0b:ce:58:b7:be:4e:30:3e:23:55:4d:
                    3c:b9:12:37:6a:82:dc:40:44:da:c8:da:89:9e:bb:
                    12:6d:a3:23:31:cb:6d:a0:52:a8:44:82:55:16:5f:
                    2b:bd:d5:ea:e7:4c:5c:00:01:f4:e2:65:c2:b9:16:
                    cf:a6:c5:b8:f8:fb:a4:70:73:04:57:51:aa:df:6f:
                    58:55:e5:e9:38:8a:e7:8c:d6:ee:a4:71:9b:4c:cc:
                    bd:94:22:00:c7:3e:68:bd:39:12:d9:15:93:8e:95:
                    a4:88:7c:73:99:ff:75:9c:42:04:c7:af:0d:9c:fc:
                    81:79:83:0e:c2:2e:3d:63:2e:a9:67:07:23:e1:a8:
                    58:67:d1:e6:c9:74:d0:fb:d6:c9:e1:1c:75:17:39:
                    9b:80:09:74:b5:5a:e5:76:5b:e6:2c:a7:e0:a0:29:
                    c3:1e:f3:64:26:8c:cb:a1:a8:80:79:52:9a:f2:93:
                    a6:6e:14:3f:d8:0e:0c:06:28:86:13:20:25:e8:69:
                    35:53:33
                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:
                65:9E:85:3B:4E:C6:8D:95:80:4C:DD:53:EC:BE:12:27:19:71:3B:29
            X509v3 Authority Key Identifier:
                keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6

            Authority Information Access:
                OCSP - URI:http://r3.o.lencr.org
                CA Issuers - URI:http://r3.i.lencr.org/

            X509v3 Subject Alternative Name:
                DNS:secclo.eu, DNS:www.secclo.eu
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
                Policy: 1.3.6.1.4.1.44947.1.1.1
                  CPS: http://cps.letsencrypt.org

            CT Precertificate SCTs:
```

```
Signed Certificate Timestamp:
    Version   : v1 (0x0)
    Log ID    : 7A:32:8C:54:D8:B7:2D:B6:20:EA:38:E0:52:1E:E9:84:
                16:70:32:13:85:4D:3B:D2:2B:C1:3A:57:A3:52:EB:52
    Timestamp : Oct 16 23:11:41.820 2022 GMT
    Extensions: none
    Signature : ecdsa-with-SHA256
                30:45:02:20:24:7B:A0:C8:B0:9E:63:44:A5:E2:15:78:
                92:8E:E1:17:50:0B:2C:5A:59:9C:BD:33:57:FE:5E:28:
                9F:FE:FE:50:02:21:00:9B:21:65:7E:19:CA:D2:D0:5A:
                30:9B:37:48:6F:E8:BD:84:2F:21:71:2D:F7:F9:C9:D5:
                F3:64:52:43:02:AA:9F
Signed Certificate Timestamp:
    Version   : v1 (0x0)
    Log ID    : AD:F7:BE:FA:7C:FF:10:C8:8B:9D:3D:9C:1E:3E:18:6A:
                B4:67:29:5D:CF:B1:0C:24:CA:85:86:34:EB:DC:82:8A
    Timestamp : Oct 16 23:11:41.934 2022 GMT
    Extensions: none
    Signature : ecdsa-with-SHA256
                30:45:02:21:00:DE:4E:F8:56:54:86:BF:2D:A9:54:F0:
                57:00:33:2F:6D:AF:6F:7C:8B:34:B0:84:37:61:DF:B1:
                4D:9F:E5:7D:DF:02:20:1C:4A:EF:69:8C:B8:13:BF:78:
                4B:99:5E:86:92:47:7E:90:CB:6A:C4:90:46:51:9B:73:
                8E:7A:7D:FA:45:86:1B
Signature Algorithm: sha256WithRSAEncryption
     92:67:21:7b:19:92:d5:8d:8c:53:a6:ad:e7:c9:1a:4e:25:9c:
     9e:e1:6b:75:57:f8:f4:2e:85:2a:5d:0d:6e:7d:5f:97:d2:f5:
     6d:d2:f8:f4:90:54:d2:50:e3:6e:bb:fd:ea:a5:9b:22:ae:27:
     e4:08:20:a2:19:de:29:92:c6:a2:84:5c:d6:13:f2:d2:c6:e0:
     da:5f:9f:ae:f3:30:90:9e:4e:3e:15:e0:9b:81:7b:73:9e:99:
     0a:03:a4:f9:3e:78:c0:15:09:06:bd:8f:03:65:b1:82:7c:3c:
     ac:a1:ca:2a:fd:c8:f0:f7:43:15:1e:24:4a:30:f5:8c:b7:69:
     da:de:43:9d:67:e2:19:58:2c:09:9f:d9:0c:ec:c7:cc:1b:83:
     2b:99:f4:b3:6f:07:d4:3f:08:f0:22:c6:8c:7e:4a:42:47:d7:
     ae:6f:7c:2e:ef:b1:4b:3d:b1:49:87:57:ee:b1:a8:50:14:77:
     67:f8:75:18:3d:fe:92:b0:0d:c5:d6:7c:1d:d9:51:33:4e:ef:
     16:2e:ea:97:2e:31:19:51:a3:7f:3e:7c:ce:c9:9e:35:31:91:
     00:06:04:5b:ca:df:10:2f:66:e8:2d:b2:1a:07:40:a8:77:bf:
     f2:b4:e1:bc:4f:2a:0c:ce:a2:2a:20:0f:fc:1d:72:2b:60:60:
     4a:6d:85:3d

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            91:2b:08:4a:cf:0c:18:a7:53:f6:d6:2e:25:a7:5f:5a
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Internet Security Research Group, CN = ISRG Root X1
        Validity
            Not Before: Sep  4 00:00:00 2020 GMT
            Not After : Sep 15 16:00:00 2025 GMT
        Subject: C = US, O = Let's Encrypt, CN = R3
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:bb:02:15:28:cc:f6:a0:94:d3:0f:12:ec:8d:55:
                    92:c3:f8:82:f1:99:a6:7a:42:88:a7:5d:26:aa:b5:
                    2b:b9:c5:4c:b1:af:8e:6b:f9:75:c8:a3:d7:0f:47:
                    94:14:55:35:57:8c:9e:a8:a2:39:19:f5:82:3c:42:
                    a9:4e:6e:f5:3b:c3:2e:db:8d:c0:b0:5c:f3:59:38:
                    e7:ed:cf:69:f0:5a:0b:1b:be:c0:94:24:25:87:fa:
                    37:71:b3:13:e7:1c:ac:e1:9b:ef:db:e4:3b:45:52:
                    45:96:a9:c1:53:ce:34:c8:52:ee:b5:ae:ed:8f:de:
                    60:70:e2:a5:54:ab:b6:6d:0e:97:a5:40:34:6b:2b:
                    d3:bc:66:eb:66:34:7c:fa:6b:8b:8f:57:29:99:f8:
                    30:17:5d:ba:72:6f:fb:81:c5:ad:d2:86:58:3d:17:
                    c7:e7:09:bb:f1:2b:f7:86:dc:c1:da:71:5d:d4:46:
                    e3:cc:ad:25:c1:88:bc:60:67:75:66:b3:f1:18:f7:
                    a2:5c:e6:53:ff:3a:88:b6:47:a5:ff:13:18:ea:98:
                    09:77:3f:9d:53:f9:cf:01:e5:f5:a6:70:17:14:af:
                    63:a4:ff:99:b3:93:9d:dc:53:a7:06:fe:48:85:1d:
                    a1:69:ae:25:75:bb:13:cc:52:03:f5:ed:51:a1:8b:
                    db:15
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, TLS Web Server Authentication
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Subject Key Identifier:
                14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6
            X509v3 Authority Key Identifier:
                keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E

            Authority Information Access:
                CA Issuers - URI:http://x1.i.lencr.org/

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://x1.c.lencr.org/
```

```
        X509v3 Certificate Policies:
            Policy: 2.23.140.1.2.1
            Policy: 1.3.6.1.4.1.44947.1.1.1

    Signature Algorithm: sha256WithRSAEncryption
         85:ca:4e:47:3e:a3:f7:85:44:85:bc:d5:67:78:b2:98:63:ad:
         75:4d:1e:96:3d:33:65:72:54:2d:81:a0:ea:c3:ed:f8:20:bf:
         5f:cc:b7:70:00:b7:6e:3b:f6:5e:94:de:e4:20:9f:a6:ef:8b:
         b2:03:e7:a2:b5:16:3c:91:ce:b4:ed:39:02:e7:7c:25:8a:47:
         e6:65:6e:3f:46:f4:d9:f0:ce:94:2b:ee:54:ce:12:bc:8c:27:
         4b:b8:c1:98:2f:a2:af:cd:71:91:4a:08:b7:c8:b8:23:7b:04:
         2d:08:f9:08:57:3e:83:d9:04:33:0a:47:21:78:09:82:27:c3:
         2a:c8:9b:b9:ce:5c:f2:64:c8:c0:be:79:c0:4f:8e:6d:44:0c:
         5e:92:bb:2e:f7:8b:10:e1:e8:1d:44:29:db:59:20:ed:63:b9:
         21:f8:12:26:94:93:57:a0:1d:65:04:c1:0a:22:ae:10:0d:43:
         97:a1:18:1f:7e:e0:e0:86:37:b5:5a:b1:bd:30:bf:87:6e:2b:
         2a:ff:21:4e:1b:05:c3:f5:18:97:f0:5e:ac:c3:a5:b8:6a:f0:
         2e:bc:3b:33:b9:ee:4b:de:cc:fc:e4:af:84:0b:86:3f:c0:55:
         43:36:f6:68:e1:36:17:6a:8e:99:d1:ff:a5:40:a7:34:b7:c0:
         d0:63:39:35:39:75:6e:f2:ba:76:c8:93:02:e9:a9:4b:6c:17:
         ce:0c:02:d9:bd:81:fb:9f:b7:68:d4:06:65:b3:82:3d:77:53:
         f8:8e:79:03:ad:0a:31:07:75:2a:43:d8:55:97:72:c4:29:0e:
         f7:c4:5d:4e:c8:ae:46:84:30:d7:f2:85:5f:18:a1:79:bb:e7:
         5e:70:8b:07:e1:86:93:c3:b9:8f:dc:61:71:25:2a:af:df:ed:
         25:50:52:68:8b:92:dc:e5:d6:b5:e3:da:7d:d0:87:6c:84:21:
         31:ae:82:f5:fb:b9:ab:c8:89:17:3d:e1:4c:e5:38:0e:f6:bd:
         2b:bd:96:81:14:eb:d5:db:3d:20:a7:7e:59:d3:e2:f8:58:f9:
         5b:b8:48:cd:fe:5c:4f:16:29:fe:1e:55:23:af:c8:11:b0:8d:
         ea:7c:93:90:17:2f:fd:ac:a2:09:47:46:3f:f0:e9:b0:b7:ff:
         28:4d:68:32:d6:67:5e:1e:69:a3:93:b8:f5:9d:8b:2f:0b:d2:
         52:43:a6:6f:32:57:65:4d:32:81:df:38:53:85:5d:7e:5d:66:
         29:ea:b8:dd:e4:95:b5:cd:b5:56:12:42:cd:c4:4e:c6:25:38:
         44:50:6d:ec:ce:00:55:18:fe:e9:49:64:d4:4e:ca:97:9c:b4:
         5b:c0:73:a8:ab:b8:47:c2

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            40:01:77:21:37:d4:e9:42:b8:ee:76:aa:3c:64:0a:b7
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: O = Digital Signature Trust Co., CN = DST Root CA X3
        Validity
            Not Before: Jan 20 19:14:03 2021 GMT
            Not After : Sep 30 18:14:03 2024 GMT
        Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:ad:e8:24:73:f4:14:37:f3:9b:9e:2b:57:28:1c:
                    87:be:dc:b7:df:38:90:8c:6e:3c:e6:57:a0:78:f7:
                    75:c2:a2:fe:f5:6a:6e:f6:00:4f:28:db:de:68:86:
                    6c:44:93:b6:b1:63:fd:14:12:6b:bf:1f:d2:ea:31:
                    9b:21:7e:d1:33:3c:ba:48:f5:dd:79:df:b3:b8:ff:
                    12:f1:21:9a:4b:c1:8a:86:71:69:4a:66:66:6c:8f:
                    7e:3c:70:bf:ad:29:22:06:f3:e4:c0:e6:80:ae:e2:
                    4b:8f:b7:99:7e:94:03:9f:d3:47:97:7c:99:48:23:
                    53:e8:38:ae:4f:0a:6f:83:2e:d1:49:57:8c:80:74:
                    b6:da:2f:d0:38:8d:7b:03:70:21:1b:75:f2:30:3c:
                    fa:8f:ae:dd:da:63:ab:eb:16:4f:c2:8e:11:4b:7e:
                    cf:0b:e8:ff:b5:77:2e:f4:b2:7b:4a:e0:4c:12:25:
                    0c:70:8d:03:29:a0:e1:53:24:ec:13:d9:ee:19:bf:
                    10:b3:4a:8c:3f:89:a3:61:51:de:ac:87:07:94:f4:
                    63:71:ec:2e:e2:6f:5b:98:81:e1:89:5c:34:79:6c:
                    76:ef:3b:90:62:79:e6:db:a4:9a:2f:26:c5:d0:10:
                    e1:0e:de:d9:10:8e:16:fb:b7:f7:a8:f7:c7:e5:02:
                    07:98:8f:36:08:95:e7:e2:37:96:0d:36:75:9e:fb:
                    0e:72:b1:1d:9b:bc:03:f9:49:05:d8:81:dd:05:b4:
                    2a:d6:41:e9:ac:01:76:95:0a:0f:d8:df:d5:bd:12:
                    1f:35:2f:28:17:6c:d2:98:c1:a8:09:64:77:6e:47:
                    37:ba:ce:ac:59:5e:68:9d:7f:72:d6:89:c5:06:41:
                    29:3e:59:3e:dd:26:f5:24:c9:11:a7:5a:a3:4c:40:
                    1f:46:a1:99:b5:a7:3a:51:6e:86:3b:9e:7d:72:a7:
                    12:05:78:59:ed:3e:51:78:15:0b:03:8f:8d:d0:2f:
                    05:b2:3e:7b:4a:1c:4b:73:05:12:fc:c6:ea:e0:50:
                    13:7c:43:93:74:b3:ca:74:e7:8e:1f:01:08:d0:30:
                    d4:5b:71:36:b4:07:ba:c1:30:30:5c:48:b7:82:3b:
                    98:a6:7d:60:8a:a2:a3:29:82:cc:ba:bd:83:04:1b:
                    a2:83:03:41:a1:d6:05:f1:1b:c2:b6:f0:a8:7c:86:
                    3b:46:a8:48:2a:88:dc:76:9a:76:bf:1f:6a:a5:3d:
                    19:8f:eb:38:f3:64:de:c8:2b:0d:0a:28:ff:f7:db:
                    e2:15:42:d4:22:d0:27:5d:e1:79:fe:18:e7:70:88:
                    ad:4e:e6:d9:8b:3a:c6:dd:27:51:6e:ff:bc:64:f5:
                    33:43:4f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            Authority Information Access:
                CA Issuers - URI:http://apps.identrust.com/roots/dstrootcax3.p7c
```

```
        X509v3 Authority Key Identifier:
            keyid:C4:A7:B1:A4:7B:2C:71:FA:DB:E1:4B:90:75:FF:C4:15:60:85:89:10

        X509v3 Certificate Policies:
            Policy: 2.23.140.1.2.1
            Policy: 1.3.6.1.4.1.44947.1.1.1
              CPS: http://cps.root-x1.letsencrypt.org

        X509v3 CRL Distribution Points:

            Full Name:
              URI:http://crl.identrust.com/DSTROOTCAX3CRL.crl

        X509v3 Subject Key Identifier:
            79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E
Signature Algorithm: sha256WithRSAEncryption
     0a:73:00:6c:96:6e:ff:0e:52:d0:ae:dd:8c:e7:5a:06:ad:2f:
     a8:e3:8f:bf:c9:0a:03:15:50:c2:e5:6c:42:bb:6f:9b:f4:b4:
     4f:c2:44:88:08:75:cc:eb:07:9b:14:62:6e:78:de:ec:27:ba:
     39:5c:f5:a2:a1:6e:56:94:70:10:53:b1:bb:e4:af:d0:a2:c3:
     2b:01:d4:96:f4:c5:20:35:33:f9:d8:61:36:e0:71:8d:b4:b8:
     b5:aa:82:45:95:c0:f2:a9:23:28:e7:d6:a1:cb:67:08:da:a0:
     43:2c:aa:1b:93:1f:c9:de:f5:ab:69:5d:13:f5:5b:86:58:22:
     ca:4d:55:e4:70:67:6d:c2:57:c5:46:39:41:cf:8a:58:83:58:
     6d:99:fe:57:e8:36:0e:f0:0e:23:aa:fd:88:97:d0:e3:5c:0e:
     94:49:b5:b5:17:35:d2:2e:bf:4e:85:ef:18:e0:85:92:eb:06:
     3b:6c:29:23:09:60:dc:45:02:4c:12:18:3b:e9:fb:0e:de:dc:
     44:f8:58:98:ae:ea:bd:45:45:a1:88:5d:66:ca:fe:10:e9:6f:
     82:c8:11:42:0d:fb:e9:ec:e3:86:00:de:9d:10:e3:38:fa:a4:
     7d:b1:d8:e8:49:82:84:06:9b:2b:e8:6b:4f:01:0c:38:77:2e:
     f9:dd:e7:39
```