Leveraging DNSSEC in Digital Identity

We're missing DNS/DNSSEC support for finding, identifying, and authenticating "Digital Identity Trust Registries". Here is our proposal for solving this.

By leveraging TLSA records, PKI, and the existing DNS/DNSSEC infrastructure, it is possible to validate the authenticity and integrity of an end entity as well as its issuer/authority, simply by performing a handful of DNS queries and manipulating the results therein.

To perform a DNS lookup and retrieve the corresponding TLSA records to verify an end entity (a device in this case), we perform a dig query with:

- **dig 5672476c-e9aa-4aa3-9cfd-2aef76f44f0f._device.iotregistry.ca tlsa +dnssec +multi**

```
jesse@CIRA-20190001:/c/Users/Jesse.Carter$ dig 5672476c-e9aa-4aa3-9cfd-2aef76f44f0f._device.iotregistry.ca tlsa +dnssec +multi

; <<>> DiG 9.16.1-Ubuntu <<>> 5672476c-e9aa-4aa3-9cfd-2aef76f44f0f._device.iotregistry.ca tlsa +dnssec +multi
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56618
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4000
;; QUESTION SECTION:
;5672476c-e9aa-4aa3-9cfd-2aef76f44f0f._device.iotregistry.ca. IN        TLSA
```

Figure 1.1 Device dig query Question Section

This query returns 3 important answers:

1. The first answer in the dig query in **Figure 1.2** contains the TLSA record usage 3 0 1 corresponding to our IoT device. This TLSA usage indicates the record corresponds to an end entity, and we are including an unsalted SHA256 hash of its binary encoded certificate data. This can then be used by another entity to validate that the certificate presented by a device claiming to be **5672476c-e9aa-4aa3-9cfd-2aef76f44f0f** is authoritatively valid by checking that the SHA256 hash of the presented certificate matches its TLSA record.
2. For the sake of demonstration, we have included a TLSA record of type 3 0 0 for the device. See the second answer in **Figure 1.2**. In an operational setting, posting the device certificate in full would not be necessary. However, in this case by posting the device certificate we can allow readers to follow along with the demo themselves. Included later in this document are the steps necessary to convert this hex encoded certificate data back into a PEM formatted cert, but for brevity we have presented the decoded cert below (see **Figure 2**)
3. The third and final answer in the query is the RRSIG corresponding to the **5672476c-e9aa-4aa3-9cfd-2aef76f44f0f._device.iotregistry.ca** record set (see **Figure 1.2**), indicating that zone is secured with DNSSEC.

```
;; ANSWER SECTION:
5672476c-e9aa-4aa3-9cfd-2aef76f44f0f._device.iotregistry.ca. 3600 IN TLSA 3 0 1 (
                                2ADF8C61777F73838D04FAF402992689419B67421708
                                1C9A930D64E1FF5677CE )
5672476c-e9aa-4aa3-9cfd-2aef76f44f0f._device.iotregistry.ca. 3600 IN TLSA 3 0 0 (
                                308204B8308203A0A003020102020210023O0D06092A
                                864886F70D01010B0500305B310B3009060355040613
                                0243413110300E06035504080C074F6E746172696F31
                                0D300B060355040A0C0443495241310D300B06035504
                                0B0C044C616273311C301A06035504030C13496F5420
                                526567697374727920537622043413O1E170D323230
                                373231313733353536 5A170D32333037333131373335
                                35365A307B310B3009060355040613024341311O300E
                                06035504080C074F6E746172696F310D300B06035504
                                0A0C0443495241310D300B0603550408B0C044C616273
                                313C303A06035504030C333536373234373663 2D6539
                                61612D346161332D396366642D326165663736663434
                                6630662E696F747265676973747279 2E636130820122
                                300D06092A864886F70D01010105000382010F003082
                                010A0282010100D0CF04E664F5544A04D815EA393336
                                1A4036CF09E2E543B9717CB064F3D7A599E8DEB2E6E5
                                680831DFE58F4CDB5F2592DA70C2AFE82987095EA54B
                                F865F6A8960F2720BCC67732858C32725B7968D463D6
                                54CCAC4D12CF46F755B167EF1F47F35BC91C90E58660
                                0B1034551F395163E1241E549BC49DD5A1EC38562C42
                                81686EB6DB79ED7EBD14353C8D429D90ED844AB2F45F
                                38EA51699E2916C43AB8FB712B3EA59F3A4D1EB1F5EE
                                F5BB0765A347FA0BA95EB9F33F736FB8B32EEF22D2C7
                                9C3D54C001E0FC78F61544D1A11A0FD4DF06B595DCA8
                                E38A726CE825A9C13C872707BB7B71E9865F3B71A711
                                C94792C765EDFDD8E077B02949FC1DCB8DD68A1A9302
                                03010001A382016430820160300906035 51D13040230
                                00301106096086480186F8420101040403020 5A03033
                                06096086480186F842010D042616244F70656E53534C
                                2047656E65726174656420436C69656E742043657274
                                6966696361746530 1D0603551D0E04160414EA72BC85
                                779CFD67D343F8AE097DC142607070DC301F0603551D
                                23041830168014F8570ED695CE40706FD794970E6414
                                0E85B55FE0300E0603551D0F0101FF0404030205E030
                                1D0603551D250416301406082B060105050703020608
                                2B0601050507030430819B0603551D11048193308190
                                823B3536373234373663 2D653961612D346161332D39
                                6366642D326165663736663434 6630662E5F64657669
                                63652E696F747265676973747279 2E63618239353637
                                32343736632D653961612D346161332D396366642D32
                                6165663736663434 6630662E5F6465766963652E7061
                                726B6F736572762E636181166A6163717565732E6C61
                                746F757240636972612E6361300D06092A864886F70D
                                01010B0500038201010 01E47C2C6E1D4718E408C0B7D
                                A149A4BECDDB36178B738A8532DED4C54A9421A0FDE7
                                BB22BD0F804E476D6817CD91E0EFA575AA11A85A5D08
                                6DF553B0C4F7092C0D281C534FBEAE7094E3E2262600
                                A91376A23EA2C7DF2889D9BB74FD48C9221FA7E348E4
                                F3889F8B28102F09DEB6FBF5BF36637AC2FDDCC3A16A
                                CBA180D878323DE79BED7CCDE7D762A3CC3DF94C2B30
                                AAE5585D9A03C76C1F2067767063F7EDE5A7CEC7FEAC
                                9DCCBE5141C097FA22C2B6C3390FA3E184D856893556
                                D26A2CDB50F39B24334156334 33A30DB96CE88231EF7
                                5ADA6F0274217AA36263F2DF7821296BBDD783372CD2
                                CDA7CAE14C9C43700E07EE935249524312AEF266B9FF
                                773E )
5672476c-e9aa-4aa3-9cfd-2aef76f44f0f._device.iotregistry.ca. 3600 IN RRSIG TLSA 13 4 3600 (
                                20220804000000 20220714000000 11926 iotregistry.ca.
                                mMyryqAD7tknR6x6DPSq7SBWxs04aM+xs5lIRG/c25Wo
                                56IyxzBJsWmu5TRwMxJuFM9fBk1SvOnG/MIopIe89g== )
```

Figure 1.2 Device dig query Answer Section

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4098 (0x1002)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer:
            commonName               = IoT Registry Sub CA
            organizationalUnitName   = Labs
            organizationName         = CIRA
            stateOrProvinceName      = Ontario
            countryName              = CA
        Validity
            Not Before: Jul 21 17:35:56 2022 GMT
            Not After : Jul 31 17:35:56 2023 GMT
        Subject:
            commonName               = 5672476c-e9aa-4aa3-9cfd-2aef76f44f0f.iotregistry.ca
            organizationalUnitName   = Labs
            organizationName         = CIRA
            stateOrProvinceName      = Ontario
            countryName              = CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d0:cf:04:e6:64:f5:54:4a:04:d8:15:ea:39:33:
                    36:1a:40:36:cf:09:e2:e5:43:b9:71:7c:b0:64:f3:
                    d7:a5:99:e8:de:b2:e6:e5:68:08:31:df:e5:8f:4c:
                    db:5f:25:92:da:70:c2:af:e8:29:87:09:5e:a5:4b:
                    f8:65:f6:a8:96:0f:27:20:bc:c6:77:32:85:8c:32:
                    72:5b:79:68:d4:63:d6:54:cc:ac:4d:12:cf:46:f7:
                    55:b1:67:ef:1f:47:f3:5b:c9:1c:90:e5:86:60:0b:
                    10:34:55:1f:39:51:63:e1:24:1e:54:9b:c4:9d:d5:
                    a1:ec:38:56:2c:42:81:68:6e:b6:db:79:ed:7e:bd:
                    14:35:3c:8d:42:9d:90:ed:84:4a:b2:f4:5f:38:ea:
                    51:69:9e:29:16:c4:3a:b8:fb:71:2b:3e:a5:9f:3a:
                    4d:1e:b1:f5:ee:f5:bb:07:65:a3:47:fa:0b:a9:5e:
                    b9:f3:3f:73:6f:b8:b3:2e:ef:22:d2:c7:9c:3d:54:
                    c0:01:e0:fc:78:f6:15:44:d1:a1:1a:0f:d4:df:06:
                    b5:95:dc:a8:e3:8a:72:6c:e8:25:a9:c1:3c:87:27:
                    07:bb:7b:71:e9:86:5f:3b:71:a7:11:c9:47:92:c7:
                    65:ed:fd:d8:e0:77:b0:29:49:fc:1d:cb:8d:d6:8a:
                    1a:93
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            Netscape Comment:
                OpenSSL Generated Client Certificate
            X509v3 Subject Key Identifier:
                EA:72:BC:85:77:9C:FD:67:D3:43:F8:AE:09:7D:C1:42:60:70:70:DC
            X509v3 Authority Key Identifier:
                keyid:F8:57:0E:D6:95:CE:40:70:6F:D7:94:97:0E:64:14:0E:85:B5:5F:E0

            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection
            X509v3 Subject Alternative Name:
                DNS:5672476c-e9aa-4aa3-9cfd-2aef76f44f0f._device.iotregistry.ca, DNS:5672476c-e9aa-4aa3-9cfd-2aef76f44f0f._device.parkoserv.ca, email:jacques.latour@cira.ca
```

```
Signature Algorithm: sha256WithRSAEncryption
    1e:47:c2:c6:e1:d4:71:8e:40:8c:0b:7d:a1:49:a4:be:cd:db:
    36:17:8b:73:8a:85:32:de:d4:c5:4a:94:21:a0:fd:e7:bb:22:
    bd:0f:80:4e:47:6d:68:17:cd:91:e0:ef:a5:75:aa:11:a8:5a:
    5d:08:6d:f5:53:b0:c4:f7:09:2c:0d:28:1c:53:4f:be:ae:70:
    94:e3:e2:26:26:00:a9:13:76:a2:3e:a2:c7:df:28:89:d9:bb:
    74:fd:48:c9:22:1f:a7:e3:48:e4:f3:88:9f:8b:28:10:2f:09:
    de:b6:fb:f5:bf:36:63:7a:c2:fd:dc:c3:a1:6a:cb:a1:80:d8:
    78:32:3d:e7:9b:ed:7c:cd:e7:d7:62:a3:cc:3d:f9:4c:2b:30:
    aa:e5:58:5d:9a:03:c7:6c:1f:20:67:76:70:63:f7:ed:e5:a7:
    ce:c7:fe:ac:9d:cc:be:51:41:c0:97:fa:22:c2:b6:c3:39:0f:
    a3:e1:84:d8:56:89:35:56:d2:6a:2c:db:50:f3:9b:24:33:41:
    56:33:43:3a:30:db:96:ce:88:23:1e:f7:5a:da:6f:02:74:21:
    7a:a3:62:63:f2:df:78:21:29:6b:bd:d7:83:37:2c:d2:cd:a7:
    ca:e1:4c:9c:43:70:0e:07:ee:93:52:49:52:43:12:ae:f2:66:
    b9:ff:77:3e
```

Figure 2.0 Device certificate decoded

Simply validating the end entity and its certificate is not enough, we must validate the issuer/authority of that end entity, which in this case is **iotregistry.ca**.

This is accomplished by performing a DNS lookup on the domain **iotregistry.ca** and retrieving the TLSA records associated it. Two TLSA records with usage 0 0 0 will be returned in the response, one containing the root certificate for **iotregistry.ca**, and one containing the sub certificate for **iotregistry.ca**. With the root and sub certificates now in hand, we can validate the certificate chain from the device certificate all the way to the root certificate of the issuer, completing the cryptographic chain of trust between the end entity and its issuer/authority.

To perform a DNS lookup to retrieve the corresponding TLSA records and certificates to validate the cryptographic chain of trust, we perform a dig query on **iotregistry.ca**:

- **dig iotregistry.ca tlsa +dnssec+multi**

```
jesse@CIRA-20190001:/c/Users/Jesse.Carter$ dig iotregistry.ca tlsa +dnssec +multi

; <<>> DiG 9.16.1-Ubuntu <<>> iotregistry.ca tlsa +dnssec +multi
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2974
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4000
;; QUESTION SECTION:
;iotregistry.ca.                IN TLSA
```

Figure 3.1 Issuer dig query question section

This query returns 3 important answers:

1. The first answer to our query is the IoT Registry sub certificate (see **Figure 3.2**). The certificate content is hexadecimal (DER) encoded as required by https://datatracker.ietf.org/doc/html/rfc6698.
2. The second answer to our query is the IoT Registry root certificate (see **Figure 3.3**).
3. The third and final answer in the query is the RRSIG corresponding to the **iotregistry.ca** record set, indicating that zone is secured with DNSSEC (see **Figure 3.3**)

```
;; ANSWER SECTION:
iotregistry.ca.         3600 IN TLSA 0 0 0 (
                                308203B53082029DA003020102020210003 00D06092A
                                864886F70D01010B0500305C310B3009060355040613
                                0243413110300E06035504080C074F6E746172696F31
                                0D300B060355040A0C0443495241310D300B06035504
                                0B0C044C616273311D301B06035504030C14496F5420
                                526567697374727920526F6F74204341301E170D3232
                                303731353138333534345A170D333230373132313833
                                3534345A305B310B300906035504061302434131103 0
                                0E06035504080C074F6E746172696F310D300B060355
                                040A0C0443495241310D300B060355040B0C044C6162
                                73311C301A06035504030C13496F5420526567697374
                                72792053756220434130820122300D06092A864886F7
                                0D010101050003820 10F003082010A0282010100CCF9
                                C2730BE02B7A6A68D32D15078D5DBF8BA8351F529C82
                                5AD407FA814C58F52300AD2A0D3A6A9C6D52381B9FCB
                                3C4BD9CB5B5FAFC9935298D77E0DA74F62768DEA3092
                                35D6402374EC921241727ABAFF6FD8AB0EEA26F97C11
                                AF680E5F879A78664CA9A267BD36F4E01374D40498D2
                                BDAAF1CBDA9A5B7233AC960103C3F372FD92942A441C
                                5029EA4E17429CF6DBA9E6117B7561795DDD07960CC9
                                0A8DAD5F8DA64F6FC8E8071E28F2039AC04E2B746D5C
                                64A1515A295B30E3C396E5327F9B6FDC36768C683EB9
                                27E8497E77F822CCF33117791459EAA0ABD7240DD464
                                CC8968CA27537E400C7A43EA1A1B41F3BE7A0B17EA3A
                                524026BE75CBE70E2E0756F10203010001A38181307F
                                301D0603551D0E04160414F8570ED695CE40706FD794
                                970E64140E85B55FE0301F0603551D23041830168014
                                18E08E5526B9BB490250AC7A9407FE35D7A9DB563012
                                0603551D130101FF040830060101FF020100300E0603
                                551D0F0101FF040403020186301906035 51D11041230
                                10820E696F747265676973747279 2E6361300D06092A
                                864886F70D01010B0500038201010070D637533AE741
                                72A15066A6520DE01F13882E91C94875300F56F36ECB
                                BD9F210C21D91A3120D6F685B32FD2E69F503017C968
                                6F86925D15D753161364DDCF7A3E15F06F0E86EE8867
                                21A203B01853B91619F348175B83862BA4DDDEF0EC60
                                5998B8DADA63DC0C032E6E248E34EF36D118F84C525D
                                853F70E47408529724B927EAFC86205A58B7563D2AFA
                                4CCA266D17F926B864D54D96841B481F330DDAA4DEAE
                                C2F67DF4297C2447BE63BFFE196C48C85AE6AF53B280
                                ED0659F2303B53D6A657F0ECEC1C06B4F7BCD3644865
                                92D9B17310527B4C46AE158EB20E8688BFDCC879D225
                                8B31C6B4CFDFDE065C986C45348A26AA3225F1E91C2A
                                A88D130D47E8CE )
```

Figure 3.2 Issuer dig query Answer Section Part 1

```
iotregistry.ca.         3600 IN TLSA 0 0 0 (
                                308203C4308202ACA003020102021448BB302E1E9F78
                                312998E9DA59373C3C358499A0300D06092A864886F7
                                0D01010B0500305C310B300906035504061302434131
                                10300E06035504080C074F6E746172696F310D300B06
                                0355040A0C0443495241310D300B060355040B0C044C
                                616273311D301B06035504030C14496F542052656769
                                7374727920526F6F74204341301E170D323230373135
                                3138313331335A170D343230373130313831333133 5A
                                305C310B300906035504061302434131 10300E060355
                                04080C074F6E746172696F310D300B060355040A0C04
                                43495241310D300B060355040B0C044C616273311D30
                                1B06035504030C14496F542052656769737472792052
                                6F6F74204341308201223 00D06092A864886F70D0101
                                0105000382010F003082010A0282010100C77F6F2A13
                                3F1E9FF7C5136CD9D2743FE84AC3C3AFA63923425643
                                74C21670FA40528AE4C7C1A047DDCB636891907D328B
                                FDA29C2C435DAC1B006817544FB2EAA27AD6639FB15F
                                3AAF5BEAC5D58BB1F50200AB89F2315743E9DC18A447
                                881A10630FBF7FD207AA4DCF44E2BE872412BBAA81C4
                                EF5B0DCFE020611E50ED5AC0AFFB574FA7C0C64D39C9
                                14021B5C940B9D4B95F8DBD84AAB998FAF053F8B26E2
                                428EA92F6C7371AC13F4220AFEF13296BF137FF95D85
                                C410A5CBB658770A2B8049E9E9EE12B276E4EB0227DC
                                972AC891D69D7F4776F5E37F7BC2A2751F90174E850A
                                9BFBC928808E9C8990DEB5D1714B92148E053731EFC7
                                AB8E95DAC0423E2D050203010001A37E307C301D0603
                                551D0E0416041418E08E5526B9BB490250AC7A9407FE
                                35D7A9DB56301F0603551D2304183016801418E08E55
                                26B9BB490250AC7A9407FE35D7A9DB56300F0603551D
                                130101FF040530030101FF300E0603551D0F0101FF04
                                0403020186301906035 51D1104123010820E696F7472
                                656769737472792E6361300D06092A864886F70D0101
                                0B0500038201010017BFF33253A2DFF1CD5A118A8A2E
                                7E348B1DD7EFD87DDD58508026B1E9A0638A61168B73
                                793912618DB7E09181EAB91E58AF997D9BB8CF74BBAF
                                62965F824497BFD35BCA0CD486148B0550F9C523B188
                                973AF8501A2EB5BAF918D4380320166107E73580BDCC
                                2DDC3EEDA58932EE3388954CED3AD68BF612F741325A
                                EB2BF13D44CE4479B4D48F06733810FC0541A707677E
                                46ACBD11A04C8043A3ED3078D551E2911CC68EE2CA03
                                947BEFD8CE868938D0A19D1AA1C00F5BA967E21E2400
                                4997B6D0D820AF6F7AF89E7EF653BAC981D241769063
                                53F7A4223075B6EC3A9D90E4EE772DF387DAF3779DE8
                                D488E8479B9DED2A7B55B2D0720BE41DA05CC409457D )
iotregistry.ca.         3600 IN RRSIG TLSA 13 2 3600 (
                                20220804000000 20220714000000 11926 iotregistry.ca.
                                OQTjD2HEVsjxbJgDlYljtDI9vhYH9NxSo5ac4R2EvNAm
                                7wc+nvva00IHdX7aFUu0h9cKy4rvKsR4fmTeK9Ioww== )
```

Figure 3.3 Issuer dig query Answer Section Part 2

While we now have both the root and sub certificates, they are not in a very useful format. Our first step to return them to easily useable PEM encoded certificates is to encode our hexadecimal certificate content back to base64, as required by PEM formatting (see **Figures 4.1 and 4.2**) This was accomplished using this link (https://holtstrom.com/michael/tools/hextopem.php) resulting in these outputs.

MIIDtTCCAp2gAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwXDELMAkGA1UEBhMCQ0ExEDAOBgNVBAg
MB09udGFyaW8xDTALBgNVBAoMBENJUkExDTALBgNVBAsMBExhYnMxHTAbBgNVBAMMFElvVCBSZWd
pc3RyeSBSb290IENBMB4XDTIyMDcxNTE4MzU0NFoXDTMyMDcxMjE4MzU0NFowWzELMAkGA1UEBhMC
Q0ExEDAOBgNVBAgMB09udGFyaW8xDTALBgNVBAoMBENJUkExDTALBgNVBAsMBExhYnMxHDAaBgNV
BAMME0lvVCBSZWdpc3RyeSBTdWIgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoI
BAQDM+cJzC+Arempo0y0VB41dv4uoNR9SnIJa1Af6gUxY9SMArSoNOmqcbVI4G5/LPEvZy1tfr8mTUpjXfg2
nT2J2jeowkjXWQCN07JISQXJ6uv9v2KsO6ib5fBGvaA5fh5p4Zkypome9NvTgE3TUBJjSvarxy9qaW3IzrJYBA8
Pzcv2SlCpEHFAp6k4XQpz226nmEXt1YXld3QeWDMkKja1fjaZPb8joBx4o8gOawE4rdG1cZKFRWilbMOPDlu
Uyf5tv3DZ2jGg+uSfoSX53+CLM8zEXeRRZ6qCr1yQN1GTMiWjKJ1N+QAx6Q+oaG0HzvnoLF+o6UkAmvnXL5
w4uB1bxAgMBAAGjgYEwfzAdBgNVHQ4EFgQU+FcO1pXOQHBv15SXDmQUDoW1X+AwHwYDVR0jBBgwF
oAUGOCOVSa5u0kCUKx6lAf+Ndep21YwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAYY
wGQYDVR0RBBIwEIIOaW90cmVnaXN0cnkuY2EwDQYJKoZIhvcNAQELBQADggEBAHDWN1M650FyoVBmp
lIN4B8TiC6RyUh1MA9W827LvZ8hDCHZGjEg1vaFsy/S5p9QMBfJaG+Gkl0V11MWE2Tdz3o+FfBvDobuiGch
ogOwGFO5FhnzSBdbg4YrpN3e8OxgWZi42tpj3AwDLm4kjjTvNtEY+ExSXYU/cOR0CFKXJLkn6vyGIFpYt1Y9K
vpMyiZtF/kmuGTVTZaEG0gfMw3apN6uwvZ99Cl8JEe+Y7/+GWxIyFrmr1OygO0GWfIwO1PWplfw7OwcBrT
3vNNkSGWS2bFzEFJ7TEauFY6yDoaIv9zIedIlizHGtM/f3gZcmGxFNIomqjll8ekcKqiNEw1H6M4=

Figure 4.1 iotregistry.ca sub certificate content base64

MIIDxDCCAqygAwIBAgIUS7swLh6feDEpmOnaWTc8PDWEmaAwDQYJKoZIhvcNAQELBQAwXDELMAk
GA1UEBhMCQ0ExEDAOBgNVBAgMB09udGFyaW8xDTALBgNVBAoMBENJUkExDTALBgNVBAsMBExhYn
MxHTAbBgNVBAMMFElvVCBSZWdpc3RyeSBSb290IENBMB4XDTIyMDcxNTE4MTMxM1oXDTQyMDcxMD
E4MTMxM1owXDELMAkGA1UEBhMCQ0ExEDAOBgNVBAgMB09udGFyaW8xDTALBgNVBAoMBENJUkEx
DTALBgNVBAsMBExhYnMxHTAbBgNVBAMMFElvVCBSZWdpc3RyeSBSb290IENBMIIBIjANBgkqhki
G9w0BAQEFAAOCAQ8AMIIBCgKCAQEAx39vKhM/Hp/3xRNs2dJ0P+hKw8OvpjkjQlZDdMIWcPpAUorkx8Gg
R93LY2iRkH0yi/2inCxDXawbAGgXVE+y6qJ61mOfsV86r1vqxdWLsfUCAKuJ8jFXQ+ncGKRHiBoQYw+/f9IHqk
3PROK+hyQSu6qBxO9bDc/gIGEeUO1awK/7V0+nwMZNOckUAhtclAudS5X429hKq5mPrwU/iybiQo6pL2xz
cawT9CIK/vEylr8Tf/ldhcQQpcu2WHcKK4BJ6enuErJ25OsCJ9yXKsiR1p1/R3b14397wqJ1H5AXToUKm/vJKIC
OnImQ3rXRcUuSFI4FNzHvx6uOldrAQj4tBQIDAQABo34wfDAdBgNVHQ4EFgQUGOCOVSa5u0kCUKx6lAf+N
dep21YwHwYDVR0jBBgwFoAUGOCOVSa5u0kCUKx6lAf+Ndep21YwDwYDVR0TAQH/BAUwAwEB/zAOBgN
VHQ8BAf8EBAMCAYYwGQYDVR0RBBIwEIIOaW90cmVnaXN0cnkuY2EwDQYJKoZIhvcNAQELBQADggEBAB
e/8zJTot/xzVoRiooufjSLHdfv2H3dWFCAJrHpoGOKYRaLc3k5EmGNt+CRgeq5HlivmX2buM90u69ill+CRJe/0
1vKDNSGFIsFUPnFI7GIlzr4UBoutbr5GNQ4AyAWYQfnNYC9zC3cPu2liTLuM4iVTO061ov2EvdBMlrrK/E9RM
5EebTUjwZzOBD8BUGnB2d+Rqy9EaBMgEOj7TB41VHikRzGjuLKA5R779jOhok40KGdGqHAD1upZ+IeJABJl7
bQ2CCvb3r4nn72U7rJgdJBdpBjU/eklJB1tuw6nZDk7nct84fa83ed6NSI6Eebne0qe1Wy0HIL5B2gXMQJRX0=

Figure 4.2 iotregistry.ca root certificate content base64

Now that the certificate content is base64 encoded, we need to apply PEM style formatting to them, new lines after every 64th character as well as the appropriate header and footer (see **Figures 5.1 and 5.2**). This was accomplished using this link (https://www.samltool.com/format_x509cert.php)

```
-----BEGIN CERTIFICATE-----
MIIDtTCCAp2gAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwXDELMAkGA1UEBhMCQ0Ex
EDAOBgNVBAgMB09udGFyaW8xDTALBgNVBAoMBENJUkExDTALBgNVBAsMBExhYnMx
HTAbBgNVBAMMFElvVCBSZWdpc3RyeSBSb290IENBMB4XDTIyMDcxNTE4MzU0NFoX
DTMyMDcxMjE4MzU0NFowWzELMAkGA1UEBhMCQ0ExEDAOBgNVBAgMB09udGFyaW8x
DTALBgNVBAoMBENJUkExDTALBgNVBAsMBExhYnMxHDAaBgNVBAMME0lvVCBSZWdp
c3RyeSBTdWIgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDM+cJz
C+Arempo0y0VB41dv4uoNR9SnIJa1Af6gUxY9SMArSoNOmqcbVI4G5/LPEvZy1tf
r8mTUpjXfg2nT2J2jeowkjXWQCN07JISQXJ6uv9v2KsO6ib5fBGvaA5fh5p4Zkyp
ome9NvTgE3TUBJjSvarxy9qaW3IzrJYBA8Pzcv2SlCpEHFAp6k4XQpz226nmEXt1
YXld3QeWDMkKja1fjaZPb8joBx4o8gOawE4rdG1cZKFRWilbMOPDluUyf5tv3DZ2
jGg+uSfoSX53+CLM8zEXeRRZ6qCr1yQN1GTMiWjKJ1N+QAx6Q+oaG0HzvnoLF+o6
UkAmvnXL5w4uB1bxAgMBAAGjgYEwfzAdBgNVHQ4EFgQU+FcO1pXOQHBv15SXDmQU
DoW1X+AwHwYDVR0jBBgwFoAUGOCOVSa5u0kCUKx6lAf+Ndep21YwEgYDVR0TAQH/
BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAYYwGQYDVR0RBBIwEIIOaW90cmVnaXN0
cnkuY2EwDQYJKoZIhvcNAQELBQADggEBAHDWN1M650FyoVBmplIN4B8TiC6RyUh1
MA9W827LvZ8hDCHZGjEg1vaFsy/S5p9QMBfJaG+Gkl0V11MWE2Tdz3o+FfBvDobu
iGchogOwGFO5FhnzSBdbg4YrpN3e8OxgWZi42tpj3AwDLm4kjjTvNtEY+ExSXYU/
cOR0CFKXJLkn6vyGlFpYt1Y9KvpMyiZtF/kmuGTVTZaEG0gfMw3apN6uwvZ99Cl8
JEe+Y7/+GWxlyFrmr1OygO0GWfIwO1PWplfw7OwcBrT3vNNkSGWS2bFzEFJ7TEau
FY6yDoaIv9zIedIlizHGtM/f3gZcmGxFNIomqjIl8ekcKqiNEw1H6M4=
-----END CERTIFICATE-----
```


Figure 5.1 iotregistry.ca sub certificate PEM encoded


```
-----BEGIN CERTIFICATE-----
MIIDxDCCAqygAwIBAgIUS7swLh6feDEpmOnaWTc8PDWEmaAwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCQ0ExEDAOBgNVBAgMB09udGFyaW8xDTALBgNVBAoMBENJ
UkExDTALBgNVBAsMBExhYnMxHTAbBgNVBAMMFElvVCBSZWdpc3RyeSBSb290IENB
MB4XDTIyMDcxNTE4MTMxM1oXDTQyMDcxMDE4MTMxM1owXDELMAkGA1UEBhMCQ0Ex
EDAOBgNVBAgMB09udGFyaW8xDTALBgNVBAoMBENJUkExDTALBgNVBAsMBExhYnMx
HTAbBgNVBAMMFElvVCBSZWdpc3RyeSBSb290IENBMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAx39vKhM/Hp/3xRNs2dJ0P+hKw8OvpjkjQlZDdMIWcPpA
Uorkx8GgR93LY2iRkH0yi/2inCxDXawbAGgXVE+y6qJ61mOfsV86r1vqxdWLsfUC
AKuJ8jFXQ+ncGKRHiBoQYw+/f9lHqk3PROK+hyQSu6qBxO9bDc/gIGEeUO1awK/7
V0+nwMZNOckUAhtclAudS5X429hKq5mPrwU/iybiQo6pL2xzcawT9CIK/vEylr8T
f/ldhcQQpcu2WHcKK4BJ6enuErJ25OsCJ9yXKsiR1p1/R3b14397wqJ1H5AXToUK
m/vJKICOnImQ3rXRcUuSFI4FNzHvx6uOldrAQj4tBQIDAQABo34wfDAdBgNVHQ4E
FgQUGOCOVSa5u0kCUKx6lAf+Ndep21YwHwYDVR0jBBgwFoAUGOCOVSa5u0kCUKx6
lAf+Ndep21YwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAYYwGQYDVR0R
BBIwEIIOaW90cmVnaXN0cnkuY2EwDQYJKoZIhvcNAQELBQADggEBABe/8zJTot/x
zVoRiooufjSLHdfv2H3dWFCAJrHpoGOKYRaLc3k5EmGNt+CRgeq5HlivmX2buM90
u69ill+CRJe/01vKDNSGFIsFUPnFI7GIlzr4UBoutbr5GNQ4AyAWYQfnNYC9zC3c
Pu2liTLuM4iVTO061ov2EvdBMlrrK/E9RM5EebTUjwZzOBD8BUGnB2d+Rqy9EaBM
gEOj7TB41VHikRzGjuLKA5R779jOhok40KGdGqHAD1upZ+IeJABJl7bQ2CCvb3r4
nn72U7rJgdJBdpBjU/ekIjB1tuw6nZDk7nct84fa83ed6NSI6Eebne0qe1Wy0HIL
5B2gXMQJRX0=
-----END CERTIFICATE-----
```


Figure 5.2 iotregistry.ca root certificate PEM encoded

With these certificates in an easily consumable PEM format, we can pass the certificates into a variety of tools to decode them and extract all the relevant fields and data from them (see **Figures 6.1 and 6.2**). In this case, important fields to take note of are the **Issuer** and **Subject** fields. A root certificate is usually self-signed, and then signs another certificate (a subordinate certificate) to perform signatures on its behalf. This is done to limit the usage of its private key. Another important field to note is the **Subject Alternative Name** (SAN) field in the **x509v3 extensions**. The SAN fields for both certificates match the DNS name **iotregistry.ca**, indicating that they are both linked to this domain.

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 4096 (0x1000)
  Signature Algorithm: sha256WithRSAEncryption
    Issuer:
      commonName            = IoT Registry Root CA
      organizationalUnitName   = Labs
      organizationName        = CIRA
      stateOrProvinceName     = Ontario
      countryName           = CA
    Validity
      Not Before: Jul 15 18:35:44 2022 GMT
      Not After : Jul 12 18:35:44 2032 GMT
    Subject:
      commonName            = IoT Registry Sub CA
      organizationalUnitName   = Labs
      organizationName        = CIRA
      stateOrProvinceName     = Ontario
      countryName           = CA
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
          00:cc:f9:c2:73:0b:e0:2b:7a:6a:68:d3:2d:15:07:
          8d:5d:bf:8b:a8:35:1f:52:9c:82:5a:d4:07:fa:81:
          4c:58:f5:23:00:ad:2a:0d:3a:6a:9c:6d:52:38:1b:
          9f:cb:3c:4b:d9:cb:5b:5f:af:c9:93:52:98:d7:7e:
          0d:a7:4f:62:76:8d:ea:30:92:35:d6:40:23:74:ec:
          92:12:41:72:7a:ba:ff:6f:d8:ab:0e:ea:26:f9:7c:
          11:af:68:0e:5f:87:9a:78:66:4c:a9:a2:67:bd:36:
          f4:e0:13:74:d4:04:98:d2:bd:aa:f1:cb:da:9a:5b:
          72:33:ac:96:01:03:c3:f3:72:fd:92:94:2a:44:1c:
          50:29:ea:4e:17:42:9c:f6:db:a9:e6:11:7b:75:61:
          79:5d:dd:07:96:0c:c9:0a:8d:ad:5f:8d:a6:4f:6f:
          c8:e8:07:1e:28:f2:03:9a:c0:4e:2b:74:6d:5c:64:
          a1:51:5a:29:5b:30:e3:c3:96:e5:32:7f:9b:6f:dc:
          36:76:8c:68:3e:b9:27:e8:49:7e:77:f8:22:cc:f3:
          31:17:79:14:59:ea:a0:ab:d7:24:0d:d4:64:cc:89:
          68:ca:27:53:7e:40:0c:7a:43:ea:1a:1b:41:f3:be:
          7a:0b:17:ea:3a:52:40:26:be:75:cb:e7:0e:2e:07:
          56:f1
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Subject Key Identifier:
        F8:57:0E:D6:95:CE:40:70:6F:D7:94:97:0E:64:14:0E:85:B5:5F:E0
      X509v3 Authority Key Identifier:
        keyid:18:E0:8E:55:26:B9:BB:49:02:50:AC:7A:94:07:FE:35:D7:A9:DB:56
```

```
X509v3 Basic Constraints: critical
            CA:TRUE, pathlen:0
        X509v3 Key Usage: critical
            Digital Signature, Certificate Sign, CRL Sign
        X509v3 Subject Alternative Name:
            DNS:iotregistry.ca
    Signature Algorithm: sha256WithRSAEncryption
        70:d6:37:53:3a:e7:41:72:a1:50:66:a6:52:0d:e0:1f:13:88:
        2e:91:c9:48:75:30:0f:56:f3:6e:cb:bd:9f:21:0c:21:d9:1a:
        31:20:d6:f6:85:b3:2f:d2:e6:9f:50:30:17:c9:68:6f:86:92:
        5d:15:d7:53:16:13:64:dd:cf:7a:3e:15:f0:6f:0e:86:ee:88:
        67:21:a2:03:b0:18:53:b9:16:19:f3:48:17:5b:83:86:2b:a4:
        dd:de:f0:ec:60:59:98:b8:da:da:63:dc:0c:03:2e:6e:24:8e:
        34:ef:36:d1:18:f8:4c:52:5d:85:3f:70:e4:74:08:52:97:24:
        b9:27:ea:fc:86:20:5a:58:b7:56:3d:2a:fa:4c:ca:26:6d:17:
        f9:26:b8:64:d5:4d:96:84:1b:48:1f:33:0d:da:a4:de:ae:c2:
        f6:7d:f4:29:7c:24:47:be:63:bf:fe:19:6c:48:c8:5a:e6:af:
        53:b2:80:ed:06:59:f2:30:3b:53:d6:a6:57:f0:ec:ec:1c:06:
        b4:f7:bc:d3:64:48:65:92:d9:b1:73:10:52:7b:4c:46:ae:15:
        8e:b2:0e:86:88:bf:dc:c8:79:d2:25:8b:31:c6:b4:cf:df:de:
        06:5c:98:6c:45:34:8a:26:aa:32:25:f1:e9:1c:2a:a8:8d:13:
        0d:47:e8:ce
```

Figure 6.1 iotregistry.ca sub certificate decoded

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            4b:bb:30:2e:1e:9f:78:31:29:98:e9:da:59:37:3c:3c:35:84:99:a0
    Signature Algorithm: sha256WithRSAEncryption
        Issuer:
            commonName               = IoT Registry Root CA
            organizationalUnitName   = Labs
            organizationName         = CIRA
            stateOrProvinceName      = Ontario
            countryName              = CA
        Validity
            Not Before: Jul 15 18:13:13 2022 GMT
            Not After : Jul 10 18:13:13 2042 GMT
        Subject:
            commonName               = IoT Registry Root CA
            organizationalUnitName   = Labs
            organizationName         = CIRA
            stateOrProvinceName      = Ontario
            countryName              = CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c7:7f:6f:2a:13:3f:1e:9f:f7:c5:13:6c:d9:d2:
                    74:3f:e8:4a:c3:c3:af:a6:39:23:42:56:43:74:c2:
                    16:70:fa:40:52:8a:e4:c7:c1:a0:47:dd:cb:63:68:
                    91:90:7d:32:8b:fd:a2:9c:2c:43:5d:ac:1b:00:68:
                    17:54:4f:b2:ea:a2:7a:d6:63:9f:b1:5f:3a:af:5b:
                    ea:c5:d5:8b:b1:f5:02:00:ab:89:f2:31:57:43:e9:
                    dc:18:a4:47:88:1a:10:63:0f:bf:7f:d2:07:aa:4d:
                    cf:44:e2:be:87:24:12:bb:aa:81:c4:ef:5b:0d:cf:
                    e0:20:61:1e:50:ed:5a:c0:af:fb:57:4f:a7:c0:c6:
                    4d:39:c9:14:02:1b:5c:94:0b:9d:4b:95:f8:db:d8:
                    4a:ab:99:8f:af:05:3f:8b:26:e2:42:8e:a9:2f:6c:
                    73:71:ac:13:f4:22:0a:fe:f1:32:96:bf:13:7f:f9:
```

```
            5d:85:c4:10:a5:cb:b6:58:77:0a:2b:80:49:e9:e9:
            ee:12:b2:76:e4:eb:02:27:dc:97:2a:c8:91:d6:9d:
            7f:47:76:f5:e3:7f:7b:c2:a2:75:1f:90:17:4e:85:
            0a:9b:fb:c9:28:80:8e:9c:89:90:de:b5:d1:71:4b:
            92:14:8e:05:37:31:ef:c7:ab:8e:95:da:c0:42:3e:
            2d:05
        Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Key Identifier:
            18:E0:8E:55:26:B9:BB:49:02:50:AC:7A:94:07:FE:35:D7:A9:DB:56
        X509v3 Authority Key Identifier:
            keyid:18:E0:8E:55:26:B9:BB:49:02:50:AC:7A:94:07:FE:35:D7:A9:DB:56
        X509v3 Basic Constraints: critical
            CA:TRUE
        X509v3 Key Usage: critical
            Digital Signature, Certificate Sign, CRL Sign
        X509v3 Subject Alternative Name:
            DNS:iotregistry.ca
Signature Algorithm: sha256WithRSAEncryption
    17:bf:f3:32:53:a2:df:f1:cd:5a:11:8a:8a:2e:7e:34:8b:1d:
    d7:ef:d8:7d:dd:58:50:80:26:b1:e9:a0:63:8a:61:16:8b:73:
    79:39:12:61:8d:b7:e0:91:81:ea:b9:1e:58:af:99:7d:9b:b8:
    cf:74:bb:af:62:96:5f:82:44:97:bf:d3:5b:ca:0c:d4:86:14:
    8b:05:50:f9:c5:23:b1:88:97:3a:f8:50:1a:2e:b5:ba:f9:18:
    d4:38:03:20:16:61:07:e7:35:80:bd:cc:2d:dc:3e:ed:a5:89:
    32:ee:33:88:95:4c:ed:3a:d6:8b:f6:12:f7:41:32:5a:eb:2b:
    f1:3d:44:ce:44:79:b4:d4:8f:06:73:38:10:fc:05:41:a7:07:
    67:7e:46:ac:bd:11:a0:4c:80:43:a3:ed:30:78:d5:51:e2:91:
    1c:c6:8e:e2:ca:03:94:7b:ef:d8:ce:86:89:38:d0:a1:9d:1a:
    a1:c0:0f:5b:a9:67:e2:1e:24:00:49:97:b6:d0:d8:20:af:6f:
    7a:f8:9e:7e:f6:53:ba:c9:81:d2:41:76:90:63:53:f7:a4:22:
    30:75:b6:ec:3a:9d:90:e4:ee:77:2d:f3:87:da:f3:77:9d:e8:
    d4:88:e8:47:9b:9d:ed:2a:7b:55:b2:d0:72:0b:e4:1d:a0:5c:
    c4:09:45:7d
```

Figure 6.2 iotregistry.ca root certificate decoded

We now have three certificates in hand, the end entity device certificate, the IoT Registry sub certificate, and the IoT Registry root certificate. With all three of these certificates, we can validate the cryptographic chain of trust by validating each of the signatures starting from the root certificate all the way to the end entity certificate. This can be easily accomplished by using openssl and saving each of the 3 PEM formatted certificates to a file.

Assuming the device certificate has been saved as **device-cert.pem**, the sub certificate as **iotr-sub.pem**, and the root certificate **as iotr-root.pem**, we perform an openssl verify:

- **openssl verify -CAfile iotr-root.pem -untrusted iotr-sub.pem device-cert.pem**

```
jesse@CIRA-20190001:/c/Users/Jesse.Carter/Repositories/ietf-CA/root-ca/sub/certs$ openssl verify -CAfile
iotr-root.pem -untrusted iotr-sub.pem device-cert.pem
device-cert.pem: OK
```

Figure 7.0 openssl verify

Looking at **Figure 7.0**, we can see the response of OK Indicating that the chain of trust we have just established has been ratified and validated by openssl.

However, we still have one more step. How do we know to trust **iotregistry.ca**? We have validated the chain of trust from end entity to issuer, but how do we know to trust the issuer itself? In this case, we turn to a trust registry, and the **_trustregistry** extension of the TLSA record.

Iotregistry.ca is a member of **trustregistry.ca**, a fictional Canadian operated authority validating other organizations, much in the same way that Service Ontario is ratified by the government of Ontario.

But how do we know **iotregistry.ca** is in fact a member of **trustregistry.ca**?

We can perform a dig query to validate that there is a _trustregistry TLSA record corresponding to the issuer in question:

- **dig iotregistry.ca._trustregistry.trustregistry.ca tlsa +dnssec +multi**

```
jesse@CIRA-20190001:/c/Users/Jesse.Carter$ dig iotregistry.ca._trustregistry.trustregistry.ca tlsa +dnssec +multi

; <<>> DiG 9.16.1-Ubuntu <<>> iotregistry.ca._trustregistry.trustregistry.ca tlsa +dnssec +multi
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52545
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4000
;; QUESTION SECTION:
;iotregistry.ca._trustregistry.trustregistry.ca.        IN TLSA

;; ANSWER SECTION:
iotregistry.ca._trustregistry.trustregistry.ca. 3600 IN TLSA 0 0 1 (
                                72A286E135981BB1BD7B1361B3387E4158FBABF4BBF5
                                DCBE3D6D78BB941B2CE5 )
iotregistry.ca._trustregistry.trustregistry.ca. 3600 IN RRSIG TLSA 13 5 3600 (
                                20220804000000 20220714000000 16050 trustregistry.ca.
                                SWffThGZlHnndlqI2190YTymtCa9u/DQWMhWVlsr1QKn
                                ULKo0FwXJE88ttbVZa0yKNNQQpVOL2ku8boeR8Tbrw== )

;; Query time: 43 msec
;; SERVER: 10.2.90.26#53(10.2.90.26)
;; WHEN: Tue Jul 26 15:46:43 EDT 2022
;; MSG SIZE  rcvd: 234
```

Figure 8.0 trustregistry.ca dig query

Looking at the results of our dig query, there are two important answers:

1. Looking at the answer section of **Figure 8.0,** we can see from the first record answer that we have received a SHA256 hash of a full certificate content for the domain iotregistry.ca. In this case, it corresponds to the root certificate.
2. The second and final answer in the query is the RRSIG corresponding to the **iotregistry.ca._trustregistry.trustregistry.ca** record set (see **figure 8.0**), indicating that zone is secured with DNSSEC.

Like our initial investigation of the device certificate and its corresponding TLSA record, we can now use the TLSA record **for iotregistry.ca._trustregistry.trustregistry.ca** and the hash provided with it to validate that the root certificate we used earlier is in fact the correct root certificate for **iotregistry.ca**. If we perform an unsalted SHA256 of the root certificate, it should match the hash provided in the above TLSA record exactly.

Hashing can get a little tricky. As input can differ among platforms, representations, and file systems, the output of a SHA256 hash on the same string can differ greatly even if only a single extra space character is appended to the string. For this use case, we are posting the SHA256 hash of the binary encoded certificate data, represented hexadecimally, as a single string without additional spaces, newline characters, or other formatting. See **Figure 9.0** for an example of the iotregistry.ca root certificate represented in such a fashion.

308203c4308202aca00302010202144bbb302e1e9f78312998e9da59373c3c358499a0300d06092a86488
6f70d01010b0500305c310b3009060355040613024341311030 0e06035504080c074f6e746172696f310d
300b060355040a0c0443495241310d300b060355040b0c044c616273311d301b06035504030c14496f54
2052656769737472792052 6f6f74204341301e170d323230373135313831333133 5a170d343230373130
3138313331335a305c310b3009060355040613024341311030 0e06035504080c074f6e746172696f310d3
00b060355040a0c0443495241310d300b060355040b0c044c616273311d301b06035504030c14496f542
052656769737472792052 6f6f74204341308201221300d06092a864886f70d0101010500038201 0f003082
010a0282010100c77f6f2a133f1e9ff7c5136cd9d2743fe84ac3c3afa6392342564374c21670fa40528ae4c7
c1a047ddcb636891907d328bfda29c2c435dac1b006817544fb2eaa27ad6639fb15f3aaf5beac5d58bb1f50
200ab89f2315743e9dc18a447881a10630fbf7fd207aa4dcf44e2be872412bbaa81c4ef5b0dcfe020611e50
ed5ac0affb574fa7c0c64d39c914021b5c940b9d4b95f8dbd84aab998faf053f8b26e2428ea92f6c7371ac13
f4220afef13296bf137ff95d85c410a5cbb658770a2b8049e9e9ee12b276e4eb0227dc972ac891d69d7f477
6f5e37f7bc2a2751f90174e850a9bfbc928808e9c8990deb5d1714b92148e053731efc7ab8e95dac0423e2d
050203010001a37e307c301d0603551d0e0416041418e08e5526b9bb490250ac7a9407fe35d7a9db5630
1f0603551d2304183016801418e08e5526b9bb490250ac7a9407fe35d7a9db56300f0603551d130101ff04
0530030101ff300e0603551d0f0101ff040403020186301906 03551d1104123010820e696f747265676973
7472792e6361300d06092a864886f70d01010b0500038201010017bff33253a2dff1cd5a118a8a2e7e348b
1dd7efd87ddd58508026b1e9a0638a61168b73793912618db7e09181eab91e58af997d9bb8cf74bbaf629
65f824497bfd35bca0cd486148b0550f9c523b188973af8501a2eb5baf918d4380320166107e73580bdcc2
ddc3eeda58932ee3388954ced3ad68bf612f741325aeb2bf13d44ce4479b4d48f06733810fc0541a707677
e46acbd11a04c8043a3ed3078d551e2911cc68ee2ca03947befd8ce868938d0a19d1aa1c00f5ba967e21e2
4004997b6d0d820af6f7af89e7ef653bac981d24176906353f7a4223075b6ec3a9d90e4ee772df387daf377
9de8d488e8479b9ded2a7b55b2d0720be41da05cc409457d

Figure 9.0 iotregistry.ca root certificate content hex encoded no formatting

Performing an unsalted sha256 hash of the string found in Figure 9.0 (https://emn178.github.io/online-tools/sha256.html), we get the result:

- **72a286e135981bb1bd7b1361b3387e4158fbabf4bbf5dcbe3d6d78bb941b2ce5**

From here, because the two hashes match exactly, the record hosted by **trustregistry.ca** indeed matches the root certificate of **iotregistry.ca**. While this is just a demo, in practice the chain of trust for **trustregistry.ca** would continue all the way up to the IANA/. level, and provide a traceable chain of trust from the global root all the way to the individual end entity. And thus, the entire chain is publicly accessible, validated, and traceable, all-over DNS.