

3. RSA 인증서 표준 (ITU-X.509)

다음 분석 내용은 ITU-T Recommendation X.509 | ISO/IEC 9594-8: Information Technology 권고문서중에서 X.509 인증서에 사용되는 필드들에 대한 용도를 설명한다.

가. X.509 논리적 구조

아래 그림은 openssl을 통한 X.509 인증서에 대한 구조를 보여준다.

```

C:\Windows\system32\cmd.exe
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 60004 (0xea64)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=drminside.co.kr, OU=CTP.Test.drminside.co.kr, CN=signer1.KDS.ca-admin/dnQualifier=uWiotK9UuzFiuZX27Z5w
        Subject: O=drminside.co.kr, OU=CTP.Test.drminside.co.kr, CN=device1.KDS.ca-admin/dnQualifier=QEa9t7S2jGUckrN6X2M
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (2048 bit)
        Modulus (2048 bit):
            00:df:19:9e:5b:90:2f:cf:4f:57:fd:f0:f2:89:f4:
            65:f5:0c:8e:59:8d:f9:83:ae:c9:8f:61:16:ea:47:
            11:05:de:e9:0d:0d:0a:ba:6e:0d:0f:c9:1d:b1:15:
            d7:ad:aa:13:ed:4c:84:19:3c:e3:56:e3:71:a0:39:
            53:6b:4b:6c:9a:6c:80:ff:31:37:01:2c:0a:70:47:
            58:32:3c:2b:70:93:36:6e:be:8c:85:8f:a7:20:6b:
            90:71:3c:b0:0c:ce:fe:fa:20:3a:9b:d1:f0:9a:64:
            85:05:aa:0a:8d:da:30:ee:c8:d3:a7:2c:22:6a:2a:
            8c:e9:b0:07:30:c0:37:4e:7d:6d:2e:a1:cf:1a:c8:
            08:53:da:b3:dc:24:71:06:b9:85:b3:9e:bb:a7:10:
            f7:d1:c9:52:a6:46:24:c9:99:13:08:65:d2:52:8f:
            4e:24:a8:90:4a:04:45:8c:d2:22:fe:3c:24:dc:29:
            ef:c1:b7:fa:f8:0a:15:af:0b:fb:15:63:49:45:f9:
            ac:e4:29:49:8e:80:99:6b:c4:48:00:94:b5:c6:96:
            a8:02:34:ce:5d:bd:37:c0:b5:ed:d4:8e:65:01:c0:
            e3:7f:3f:f3:d1:e2:e1:03:60:09:23:81:37:63:8f:
            aa:a5:b6:58:a2:df:2c:ed:7c:03:ac:34:75:e8:f0:
            02:ed
        Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Key Usage:
            Digital Signature, Key Encipherment, Data Encipherment
        X509v3 Basic Constraints: critical
            CA:FALSE
        X509v3 Subject Key Identifier:
            40:46:BD:B7:B4:B3:8C:65:1C:92:B3:70:5F:63:31:37:3B:09:4E:35
        X509v3 Authority Key Identifier:
            keyid:B9:60:8E:B4:AF:55:57:31:62:B9:95:F6:ED:9E:70:00:9D:2C:32:63
            DirName:/O=drminside.co.kr/OU=CTP.Test.drminside.co.kr/CN=.KDS.ca-admin/dnQualifier=2jNxRykhZqmxYcUi7Rv3
        serial:EA:62
    Signature Algorithm: sha256WithRSAEncryption
        bf:bc:8e:94:6e:3e:b1:a4:98:e5:00:b3:c8:b2:0c:3d:b0:54:
        6a:23:4e:25:73:1d:14:3d:b9:95:52:74:ea:f9:2c:60:87:b3:
        ac:74:2d:61:18:62:9d:af:03:d6:d4:18:d5:77:f4:d0:a0:c0:
        0a:76:10:7f:d6:ec:ba:7d:a9:14:ea:f2:6d:5b:f6:60:e2:29:
        a8:73:f2:8b:3f:e4:3d:e2:e6:b9:1b:84:58:dd:af:1f:f1:fb:
    
```

[그림 8] X.509 논리적 구조