# CSR Attributes

Dan Harkins

# The Intent of CSRAttrs Request

- There are many variables when issuing certificates
  - Can assume client knows everything
  - Bad client assumptions can result in issues that are hard to diagnose
- Answer important questions on what the CSR should look like
  - Which cryptosystem?
    - If ECC, then which curve?
    - If RSA, then how big a key?
  - Any requirements on hash algorithm?
  - Any other things the CA/RA requires or expects?
- Request additional information if possible
  - MAC address or Device serial number or whatever….
- Match structure of CSR/Certificate as much as possible
  - Mimic subjectPublicKeyInfo attribute structure instead of just an OID for a curve
  - Allow for stand-alone OIDs for things that stand alone, like challengePassword

# This Interpretation is In Use Today

- DPP when issuing X.509 certificates
  - Issues CSR Attributes request in DPP Config Response if no CSR
  - Subsequent DPP Config Request with CSR is passed to CA
  - Certificate is provisioned in subsequent DPP Config Response
- EST
  - My reference implementation
  - Aruba/HPE ClearPass EST support
  - Others?

# Current CSR Attrs Definition

- ASN.1 is in the eye of the beholder
  - is “simple” (Russ Housley)
  - is “rather incomprehensible” (David von Oheimb)
- Criticism
  - Under-specified and free-form
  - Attributes do not have a clear meaning
  - It’s possible to give conflicting recommendations
- Seems like people want to use them for things they weren’t intended for
  - Have RA tell the client what his alternate name is (!)

# Backup

Example CSR Attrs, CSR, and cert….

# Example CSR Attrs Request

- CA signs with p384 and wants to issue same
- Given curve, probably best to sign with SHA384
- RA wants to see challengePassword
- Add some additional informative information

ME4GCSqGSIb3DQEJBzASBgcqhkjOPQIBMQcGBSuBBAAiMCMGCSqGSIb3DQEJDjEWBgNVBAUGA1UdEQYKCZImiZPyLGQBBQYIKoZIzj0EAwM

- Which is decoded as:

SEQUENCE (4 elem)
  OBJECT IDENTIFIER 1.2.840.113549.1.9.7 challengePassword (PKCS #9)
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.10045.2.1 ecPublicKey (ANSI X9.62 public key type)
    SET (1 elem)
      OBJECT IDENTIFIER 1.3.132.0.34 secp384r1 (SECG (Certicom) named elliptic curve)
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.9.14 extensionRequest (PKCS #9 via CRMF)
    SET (3 elem)
      OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
      OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
      OBJECT IDENTIFIER 0.9.2342.19200300.100.1.5 (favorite drink)
  OBJECT IDENTIFIER 1.2.840.10045.4.3.3 ecdsaWithSHA384 (ANSI X9.62 ECDSA algorithm with SHA384)

# Which produces this CSR

```
SEQUENCE (3 elem)
  SEQUENCE (4 elem)
    INTEGER 0
    SEQUENCE (1 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String biff
    SEQUENCE (2 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.2.840.10045.2.1 ecPublicKey (ANSI X9.62 public key type)
        OBJECT IDENTIFIER 1.3.132.0.34 secp384r1 (SECG (Certicom) named elliptic curve)
      BIT STRING (776 bit) 000001000110101101111111011000001011100010011110011111111100011000000…
    [0] (2 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.2.840.113549.1.9.14 extensionRequest (PKCS #9 via CRMF)
        SET (1 elem)
          SEQUENCE (2 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
              OCTET STRING (11 byte) SMERSH-7474
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 0.9.2342.19200300.100.1.5 (Favorite Drink)
              OCTET STRING (27 byte) le vrai pastis de Marsaille
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.2.840.113549.1.9.7 challengePassword (PKCS #9)
        SET (1 elem)
          UTF8String BXsrUDzee7EIDVrqRti+lE3AqggkHAiagFKEZaWeQ5Yba3kpWeBxA0lzZ9HJRGfYss57F6iqPfit1148…
  SEQUENCE (1 elem)
    OBJECT IDENTIFIER 1.2.840.10045.4.3.3 ecdsaWithSHA384 (ANSI X9.62 ECDSA algorithm with SHA384)
  BIT STRING (816 bit) 00110000011001000000001000110000000010001011010011000110001001001111111…
    SEQUENCE (2 elem)
      INTEGER (380 bit) 133999888658897683683644723380558107696640181173726801754045706031015 9…
      INTEGER (383 bit) 154657123454904206038659807426716955001565442945816901423131704235330 4…
```

# Which produces this Certificate

```
Data:
    Version: 3 (0x2)
    Serial Number: 10 (0xa)
  Signature Algorithm: ecdsa-with-SHA384
    Issuer: C=US, ST=CA, L=La Selva Beach, O=The Industrial Lounge, CN=doorman.lounge.org
    Validity
      Not Before: Aug 25 20:45:21 2021 GMT
      Not After : Aug 23 20:45:21 2031 GMT
    Subject: CN=biff
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
        Public-Key: (384 bit)
        pub:
          04:6b:7f:60:b8:9e:7f:c6:02:67:02:e0:16:18:61:
          [snip]
        ASN1 OID: secp384r1
        NIST CURVE: P-384
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Key Usage:
        Digital Signature, Key Encipherment
      X509v3 Extended Key Usage:
        TLS Web Client Authentication, TLS Web Server Authentication
      X509v3 Subject Key Identifier:
        0E:45:32:4C:97:D3:12:AB:A3:AE:EC:31:F4:21:FA:79:12:77:AA:DD
      X509v3 Authority Key Identifier:
        DirName:/C=US/ST=CA/L=La Selva Beach/O=The Industrial Lounge/CN=doorman.lounge.org
        serial:67:A0:52:A9:5A:40:92:04:C5:A5:C2:70:F1:0F:AF:F0:79:08:CF:64
      serialNumber:
        SMERSH-7474
      favouriteDrink:
        le vrai pastis de Marsaille
  Signature Algorithm: ecdsa-with-SHA384
     30:81:87:02:42:01:69:04:f6:b3:e1:2e:7c:ed:b4:1c:5b:7d:
     [snip]
```