Data protection scheme identifier options.

- Process works as follows
  - User creates key
  - User creates certificate signing request (csr)
  - User sends csr to IHO
  - IHO signs csr, generating data server certificate
  - IHO sends certificate back to user
- When the user creates their key and csr certain fields are defined. There is no format or guidelines for these fields currently
- The fields are “permanent”. They cannot be changed without invalidating the certificate. The certificate validates the user’s key and the fields within the csr/certificate

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            96:28:2a:a9:cd:68:76:a1
    Signature Algorithm: dsa_with_SHA256
        Issuer: C=MC, ST=Some-State, O=IHO, CN= urn:mrn:iho:aa
        Validity
            Not Before: Sep 27 13:19:46 2022 GMT
            Not After : Aug  5 13:19:46 2032 GMT
        Subject: C=GB, ST=producer, O=IIC Technologies, Vancouver, CN=urn:mrn:iho:s62:iic:2C:key3
        Subject Public Key Info:
            Public Key Algorithm: dsaEncryption
                pub:
                    7b:d1:62:9e:0b:85:22:5d:7a:a7:06:02:9f:5e:9a
                P:
                    00:94:2a:c7:99:24:2f:35:1a:ed:50:75:c2:24:0e:
                Q:
                    00:b5:96:4f:27:f7:d1:e1:f9:07:c9:50:ae:c8:fa:
                    22:f1
                G:
                    00:84:f1:ae:97:cc:a6:53:f7:78:67:ab:17:ac:18:
                    eb:60
    Signature Algorithm: dsa_with_SHA256
         r:
             56:e4:ef:0c:bc:9a:b1:ad:2b:de:f4:b0:47:45:fc:
             01:df:2c:f0:92
         s:
             63:60:c6:1e:7c:78:32:08:59:84:26:6f:5a:94:06:
             01:92:ed:d6:93
```

- Focus on the fields asked for during the CSR process. These are:
  - **`Subject: C=CN, ST=ST, O=ORG, CN=FQDN`**
- The fields are part of the certificate standard X.509
- Country, State, Organisation, Common Name
- The certificate (made by IHO) contains the issuer's details (the IHO) and the subject's details (the data server). The fields define the identity of each.
- We need to form a link between the values in these fields and the identifying fields in the data (and CATALOG.XML) included in an exchange set. Datasets always contain the data producer code
- This is so that when a data server signs a dataset there is a link between the entity signing the data and the data itself.
- E.g currently IIC can sign NOAA data. Signature is valid but IIC is not the producer. This is ok but id of the producer is lost.
- Proposal
  - Suggest the following values:
    - C (Country) = **ISO Country Code of state making request**
    - ST (State or Province) = **suggest we use this as a role code**
    - O (Organisation) = **member state organisation name (text)**
    - CN (Common Name) = **IHO data producer code integer and alpha code (colon separated MRN).**

- Proposal to use an mrn for the producer code, e.g.
  - **urn:mrn:iho:S-62:GB:540 or similar (Secretariat to finalise format)**
- This allows for flexibility. It means different organisations within an IHO member state can be represented.
- The link to producer code is a hard link between data and signature.
- Roles are useful for ISO19115 and IHO might need them. Author, RENC/distributor. This list can be formed from part 17.

Why is this useful?

- It standardises the field content which are currently “free text”
- It provides a tie between data producer codes in data and in signatures in CATALOG.XML
- Producer code registry for S-100 is being tested so all producers have alphanumeric and integer codes
- Requires no change to S-100 – feeds into action to produce guidelines for operation of the data protection scheme by IHO secretariat acting as the Scheme Administrator.
- Can be explained in S-98 and input into the S-98 review process.

CSR

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=CN, ST=ST, O=ORG, CN=FQDN
        Subject Public Key Info:
            Public Key Algorithm: dsaEncryption
                pub:
                    27:04:2b:42:50:be:94:87:b7:1a:f0:9c:32:73:b0:
                    70:f4:9e:54:61:cd:04:49:2f:d3:b1:54:d2:61:90:
                    64:9d:8a:83:54:a7:ee:b9:70:d5:6a:83:72:cc:d5:
                    c8:d3:e6:2c:02:33:2d:b8:42:3a:67:fb:00:a1:10:
                    7d:a6:b4:c1:73:73:f2:c7:58:74:fa:79:4d:78:80:
                    fe:dc:a3:5b:57:0e:27:94:3e:76:37:19:58:39:30:
                    ca:f8:38:7b:a5:96:6b:b7:47:7d:2e:b2:6f:68:00:
                    c1:b3:03:e9:7a:e8:1e:79:bd:8d:00:90:3b:4d:4d:
                    9a:58:fe:ac:56:58:07:e8
                P:
                    00:e6:b5:24:fa:00:7a:fa:e0:75:2d:d6:12:74:00:
                    26:ce:1c:ef:e7:ac:a6:05:a4:57:be:b1:36:04:8b:
                    05:da:c2:6d:18:ab:d6:b5:f5:13:fd:c7:d1:bb:51:
                    3c:c9:e8:7c:d2:6a:d4:ba:57:0e:63:2d:f3:77:f3:
                    6f:48:14:4f:35:a8:8c:51:d0:5f:cd:c7:bc:86:0f:
                    cd:fa:7e:f0:f9:dc:7b:84:6a:c8:62:1a:5f:9f:68:
                    7a:f6:4b:17:b4:83:73:79:8f:09:50:95:a1:d7:33:
                    f9:5d:ac:27:66:8b:fb:db:6d:6a:b5:08:14:c5:38:
                    b3:e8:81:9a:3b:0c:7a:39:e9
                Q:
                    00:c8:9c:27:11:5b:cf:d7:20:be:f2:aa:e3:0d:9a:
                    5e:b6:7e:55:b8:87
                G:
                    45:b8:20:2a:20:d5:33:71:54:23:37:ae:3b:e3:2d:
                    dc:3a:08:6b:b5:b7:bf:d0:a5:3c:65:ef:1c:9b:a9:
                    51:02:eb:6f:0f:6a:26:74:2f:97:e3:16:4b:20:e3:
                    f6:75:62:48:15:fc:fb:5c:b2:68:dd:e6:3c:b6:a7:
                    36:31:f5:4b:40:81:45:00:13:38:25:40:e3:77:ef:
                    59:45:0e:50:a0:37:ca:b8:dd:93:5c:ea:e2:e4:27:
                    f8:fc:96:5e:7f:ba:89:2a:83:aa:1c:fa:88:1f:ce:
                    cc:04:c5:a6:24:cc:78:51:2e:f3:c1:7e:b2:ab:a5:
                    e3:9e:48:ba:06:36:68:eb
        Attributes:
            a0:00
    Signature Algorithm: dsa_with_SHA256
         r:
             19:9f:57:5e:1e:84:e8:78:aa:e5:31:3f:91:6f:c4:
             a3:88:9c:f7:ee
         s:
             02:c2:aa:bd:34:27:af:3e:c1:ce:b0:95:2c:14:
             eb:cf:4e:b9:ba
-----BEGIN CERTIFICATE REQUEST-----
MIICOjCCAfgCAQAwNzELMAkGA1UEBhMCQ04xCzAJBgNVBAgMAlNUMQwwCgYDVQQK
DANPUkcxDTALBgNVBAMMBEZRRE4wggG2MIIBKwYHKoZIzjgEATCCAR4CgYEA5rUk
+gB6+uB1LdYSdAAmzhzv56ymBaRXvrE2BIsF2sJtGKvWtfUT/cfRu1E8yeh80mrU
ulcOYy3zd/NvSBRPNaiMUdBfzce8hg/N+n7w+dx7hGrIYhpfn2h69ksXtINzeY8J
UJWh1zP5XawnZov7221qtQgUxTiz6IGaOwx6OekCFQDInCcRW8/XIL7yquMNml62
flW4hwKBgEW4ICog1TNxVCM3rjvjLdw6CGu1t7/QpTxl7xybqVEC628PaiZ0L5fj
Fksg4/Z1YkgV/Ptcsmjd5jy2pzYx9UtAgUUAEzglQON371lFDlCgN8q43ZNc6uLk
J/j8ll5/uokqg6oc+ogfzswExaYkzHhRLvPBfrKrpeOeSLoGNmjrA4GEAAKBgCcE
K0JQvpSHtxrwnDJzsHD0nlRhzQRJL9OxVNJhkGSdioNUp+65cNVqg3LM1cjT5iwC
My24Qjpn+wChEH2mtMFzc/LHWHT6eU14gP7co1tXDieUPnY3GVg5MMr4OHullmu3
R30usm9oAMGzA+l66B55vY0AkDtNTZpY/qxWWAfooAAwCwYJYIZIAW
MCwCFBmfV14ehOh4quUxP5FvxKOInPfuAhQCwqq9NCevPsHOsJUsF0
-----END CERTIFICATE REQUEST-----
```

Fields Input by applicant during CSR creation..

Key generated by applicant.

Signature of CSR, can't be changed and validates request.

Encoded version of all this information. Contents of file sent to authoriser (IHO)

Certificate

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            96:28:2a:a9:cd:68:76:a1
    Signature Algorithm: dsa_with_SHA256
        Issuer: C=MC, ST=Some-State, O=IHO, CN=IHO Scretariat/emailAddress=jp@iho.int
        Validity
            Not Before: Sep 27 13:19:46 2022 GMT
            Not After : Aug  5 13:19:46 2032 GMT
        Subject: C=GB, ST=producer, O=IIC Technologies, Vancouver, CN=urn:mrn:iho:s62:iic:2C:key3
        Subject Public Key Info:
            Public Key Algorithm: dsaEncryption
                pub:
                    7b:d1:62:
                    66:67:c8:2c:6f:f7:e8:ca:cc:1e:83:05:30:30:ab:
                    9a
                P:
                    00:94:2a:c7:99:24:2f:b2:6c:09:8b:a1:eb:b0:f8:
                    45:35
                Q:
                    00:b5:96:4f:27:f7:d1:e1:f9:07:c9:50:ae:c8:fa:
                    22:a0:90:0d:22:05:53:69:2e:dc:68:76:73:bf:52:
                    75:f5:f1
                G:
                    00:84:f1:ae:97:cc:a6:53:f7:78:67:ab:17:ac:18:
                    eb:6d:b7:7f:da:f3:e7:a4:8d:94:e4:bc:4d:01:26:
                    61:34:3a:5e:8a:19:4a:2d:14:f0:09:f1:b7:c4:81:
                    41:8f:f4:c3:8f:69:ea:37:34:9d:03:0d:bc:a9:e6:
                    ca:60
    Signature Algorithm: dsa_with_SHA256
         r:
             56:e4:ef:0c:bc:9a:b1:ad:2b:de:f4:b0:47:45:fc:
             01:df:2c:f0:92
         s:
             63:60:c6:1e:7c:78:32:08:59:84:26:6f:5a:94:06:
             01:92:ed:d6:93
-----BEGIN CERTIFICATE-----
MIIEmTCCBFcCCQCWKCqpzWh2oTALBglghkgBZQMEAwIwZDELMAkGA1UEBhMCTUMx
Z8gsb/foyswegwUwMKuaMAsGCWCGSAFlAwQDAgMvADAsAhRW5O8MvJqxrSve9LBH
RfwB3yzwkgIUY2DGHnx4MghZhCZvWpQGAZLt1pM=
-----END CERTIFICATE-----
```

IHO.x509

Subject(CN):	urn:mrn:iho:aa
Issuer(CN):	urn:mrn:iho:aa
Key:	f1:ae:97:cc:a6

```
<S100SE:StandaloneDigitalSignature>
  <S100SE:filename>CATALOG.XML</S100SE:filename>
  <S100SE:certificates>
    <S100SE:schemeAdministrator id="urn:mrn:iho:aa"/>
    <S100SE:certificate id="urn:mrn:iho:s62:iic:2C:key1" issuer="urn:mrn:iho:aa">
      MIIEkjCCBE8CCQCWK==
    </S100SE:certificate>
  </S100SE:certificates>
  <S100SE:digitalSignature id="catalog" certificateRef="urn:mrn:iho:s62:iic:2C:key1">
       MEQCID4mW4lMTtGZkL6rEUuFUqZtVsvq1yaw5FrzGz2TY5G2AiBgiLuYBZb3vkPyCY8NqIUDUlEKiSGU7xsHpIDjlKnDMw==
  </S100SE:digitalSignature>
</S100SE:StandaloneDigitalSignature>
```

CAT.SIG

```
<S100XC:certificates>
  <S100SE:schemeAdministrator id="urn:mrn:iho:aa"/>
  <S100SE:certificate id="urn:mrn:iho:s62:iic:2C:key1“ issuer="urn:mrn:iho:aa">
    MIIEkjCCBE8CCQCWKCqpzWh2nz==
  </S100SE:certificate>
</S100XC:certificates>
```

```
<S100XC:compressionFlag>true</S100XC:compressionFlag>
<S100XC:dataProtection>true</S100XC:dataProtection>
<S100XC:protectionScheme>S100p15</S100XC:protectionScheme>
  <S100XC:digitalSignatureReference>DSA</S100XC:digitalSignatureReference>
  <S100XC:digitalSignatureValue>
    <S100SE:S100_SE_DigitalSignature id="101AA00DS0020“ certificateRef="urn:mrn:iho:s62:iic:2C:key1">
       MEUCIQCd6pOj5yd9x0+tkL7rqh2BmhQyp3Vwesd5io2nxAyEJFsvsY=
    </S100SE:S100_SE_DigitalSignature>
  </S100XC:digitalSignatureValue>
  <blah>…</blah>
```

id:	urn:mrn:iho:s62:iic:2C:key3
Issuer:	urn:mrn:iho:aa
Key:	d4:ba:57:0e:63

Certificate.

fileName:	101AA00DS0020.000
Signature:	aa:1c:fa:88:1f
Key:	d4:ba:57:0e:63

Signature.

CATALOG.XML

```
<FOID>
 <AGEN>2C</AGEN>
 <FIDN>46204</FIDN>
 <FIDS>1</FIDS>
</FOID>
```

Dataset:	101AA00DS0020.000
Product:	S-101
Producer code:	IIC/2C

Dataset.

What we currently do in the exchange catalogue builder.
- User prefs store certificates, keys and name(id) of SA