\ Issues with certificate files from S64 Test Data Sets

Problem #1 – Root certificate problem
Problem #2 – “issuer” filed problem
Problem #3 – Certificates x509 version problem

Problem #1

- S-64 / IHO Test Data Sets in ECDIS (Edition 3.0(.3) – December 2020)
- Case: 2.5.4 a) Install and validate the SA certificate and/or public key
- Check:
  - UKHO.CRT: successfully installed
  - Warning SSE26 appeared
- Certificate: UKHO.CRT (Path: S-64_ENC_Encrypted_TDS/4 Authentication_Part1/Test 4a/UKHO.CRT)
- Problem: UKHO.CRT is incorrect and doesn't comply S-63.

Problem #1 – S63 compliance

- Based of **S63 Edition 1.2.1 – March** standard parts:
  - 5.2 Digital Certificates (SA Authentication)
  - 5.4.2.4 The SA Digital Certificate (X509v3) Format
- Certificate files (*.CRT) must be **root certificate** and should comply to standard **X509v3** (third version of X509)

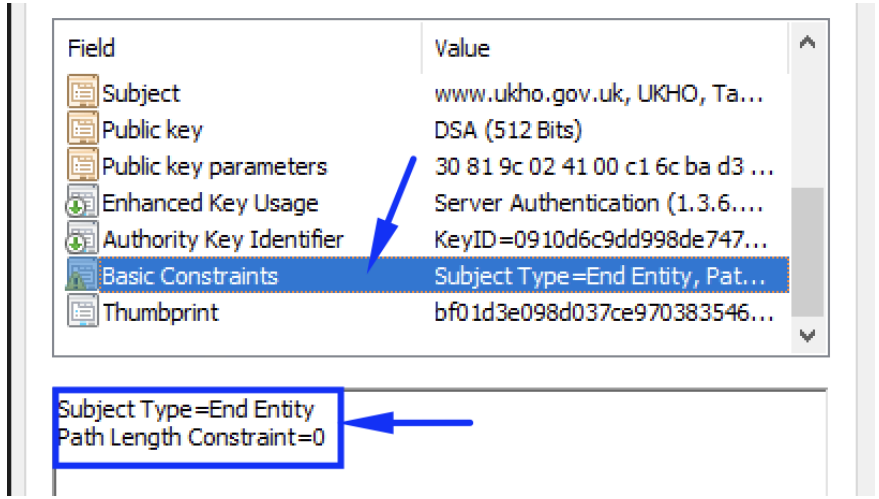
- Issue: UKHO.CRT file is **not root** certificate

Problem #1 - UKHO.CRT info

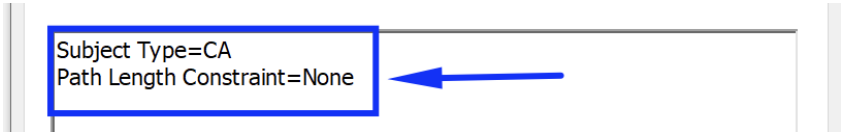
- UKHO.CRT certificate info with
  `Microsoft Windows Certificate Viewer`

> ***Certification authority** (CA)*
> *is an entity that issues digital certificates.*

Actual:



Expected:



End Entity certificate
cannot be used to sign other entities

Problem #1 - UKHO.CRT info

- UKHO.CRT certificate info with `openssl` utility
- Actual: `CA:FALSE`
- Expected: `CA:TRUE`

***Certification authority** (CA)*
is an entity that issues digital certificates.

```
Certificate:
    Data:
       Version: 3 (0x2)
       Serial Number: 869382 (0xd4406)
       Signature Algorithm: dsaWithSHA1
       Issuer: C = England, L = Taunton, O = UKHO, CN = www.ukho.gov.uk
       Validity
           Not Before: May 16 13:35:24 2002 GMT
           Not After : Aug 16 13:35:24 2010 GMT
       Subject: C = England, L = Taunton, O = UKHO, CN = www.ukho.gov.uk
       Subject Public Key Info:
        <...>
           X509v3 extensions:
               X509v3 Basic Constraints: critical
                   CA:FALSE, pathlen:0
               X509v3 Extended Key Usage:
                   TLS Web Server Authentication
               X509v3 Authority Key Identifier:
                   keyid:09:10:D6:C9:DD:99:8D:E7:47:3E:C2:89:7E


    Signature Algorithm: dsaWithSHA1
      <...>
```

Problem #1 - CA:FALSE means?

- From the official web site (https://www.openssl.org/docs/manmaster/man5/x509v3_config.html) of `openssl` utility in the Section *STANDARD EXTENSIONS / Basic Constraints* we can see:
  - A CA certificate **must** include the basicConstraints name with the **CA** parameter set to **TRUE**.
    An end-user certificate must either have CA:FALSE or omit the extension entirely.
- It means that UKHO.CRT is **not root certificate** due to **CA:FALSE** – it is not complied to S63 – therefore we cannot validate .

Problem #1 – In other S-64 test certificates

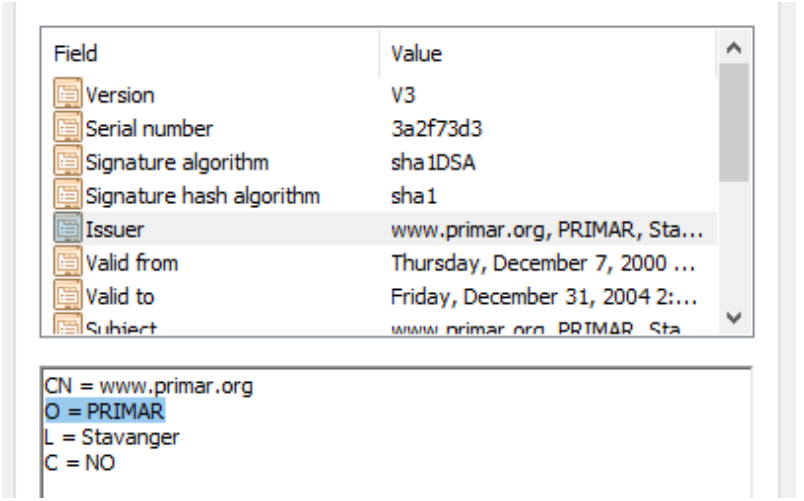
- Other Certificates from S64 data set have common problems:

- S-64_ENC_Encrypted_TDS/4 Authentication_Part1/Test 4a/UKHO.CRT
  S-64_ENC_Encrypted_TDS/5 Authentication_Part2/Test 5b/NONSA.CRT
  Issue: The field “Basic Constraints” have CA:FALSE
  Expected: CA:TRUE

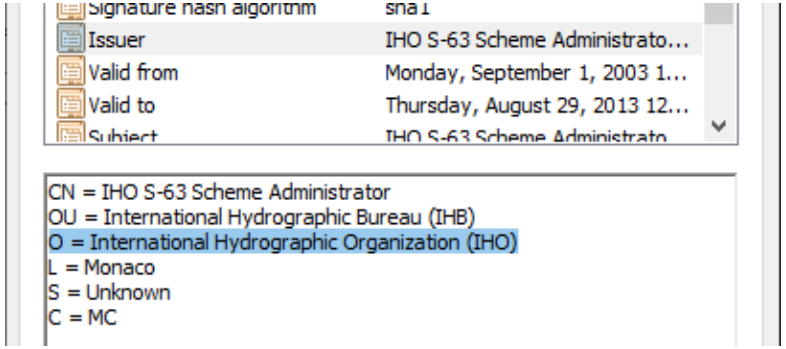
Problem #2

- Certificate IHO.CRT
  (S-64_ENC_Encrypted_TDS/4 Authentication_Part1/Test 4d/Expired/IHO.CRT)
- **Issue**: Field “Issuer” contain “PRIMAR”
- Expected: Field “Issuer” contain “IHO”
- **Reason**: Installation of Certificate with wrong field “Issuer” leads to SSE 26 warning. This is **not expected** in S64 Test 2.5.4 d) case

Actual:



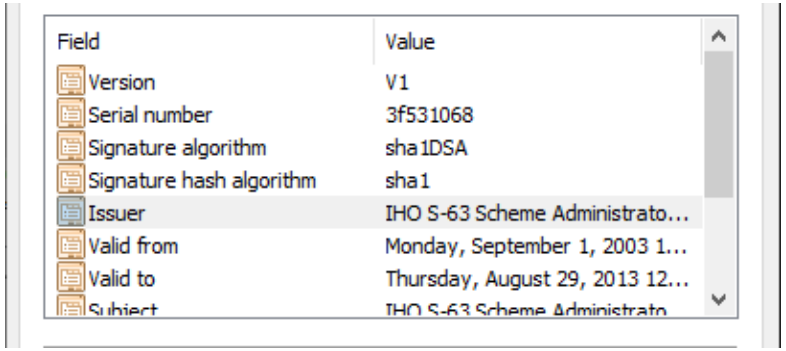
Expected: IHO (like on the below picture)



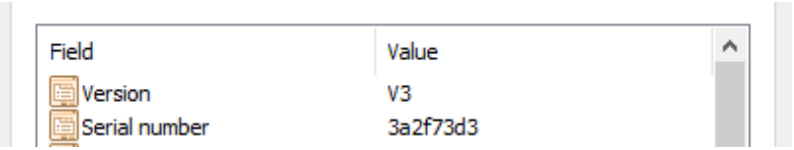
Problem #3

- S-64_ENC_Encrypted_TDS\4 Authentication_Part1\Test 4b\IHO.CRT
- S-64_ENC_Encrypted_TDS\4 Authentication_Part1\Test 4d\Current\IHO.CRT
- S-64_ENC_Encrypted_TDS\4 Authentication_Part1\Test 4d\Current\V01X01\IHO.CRT
- S-64_ENC_Encrypted_TDS\4 Authentication_Part1\Test 4e\IHO.CRT
- S-64_ENC_Encrypted_TDS\4 Authentication_Part1\Test 4f\DS1\IHO.CRT
- S-64_ENC_Encrypted_TDS\4 Authentication_Part1\Test 4f\DS2\IHO.CRT
- S-64_ENC_Encrypted_TDS\5 Authentication_Part2\Test 5a\IHO.CRT
- S-64_ENC_Encrypted_TDS\5 Authentication_Part2\Test 5b\V01X01\IHO.CRT
- S-64_ENC_Encrypted_TDS\5 Authentication_Part2\Test 5c\IHO.CRT
- S-64_ENC_Encrypted_TDS\5 Authentication_Part2\Test 5f\IHO.CRT
- S-64_ENC_Encrypted_TDS\6 ENC Decryption\Test 6a\IHO.CRT
- S-64_ENC_Encrypted_TDS\6 ENC Decryption\Test 6e\V01X01\IHO.CRT
- S-64_ENC_Encrypted_TDS\7 ENC Data Management\Test 7a\IHO.CRT
- S-64_ENC_Encrypted_TDS\8 Data Exchange Media\Test 8a\IHO.CRT

Actual:



Expected: IHO (like on the below picture)



- **Issue**: Certificates of standard X509 have first version = X509v1
- **Expects:** Certificates of standard X509 third version = X509v3
- **Reason**: S 63 standard state that third version certificates X509v3 should be installed
- (5.4.2.4 The SA Digital Certificate (X509v3) Format)