

## \ 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:**

Field	Value
Subject	www.ukho.gov.uk, UKHO, Ta...
Public key	DSA (512 Bits)
Public key parameters	30 81 9c 02 41 00 c1 6c ba d3 ...
Enhanced Key Usage	Server Authentication (1.3.6....
Authority Key Identifier	KeyID=0910d6c9dd998de747...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint	bf01d3e098d037ce970383546...

Subject Type=End Entity  
Path Length Constraint=0

**End Entity** certificate  
cannot be used to sign other entities

**Expected:**

Subject Type=CA Path Length Constraint=None
--

# 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](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:

Field	Value
Version	V3
Serial number	3a2f73d3
Signature algorithm	sha1DSA
Signature hash algorithm	sha1
Issuer	www.primar.org, PRIMAR, Sta...
Valid from	Thursday, December 7, 2000 ...
Valid to	Friday, December 31, 2004 2:...
Subject	www.primar.org, PRIMAR, Sta...

CN = www.primar.org  
O = PRIMAR  
L = Stavanger  
C = NO

Expected: IHO (like on the below picture)

Signature algorithm	sha1
Issuer	IHO S-63 Scheme Administrato...
Valid from	Monday, September 1, 2003 1...
Valid to	Thursday, August 29, 2013 12...
Subject	IHO S-63 Scheme Administrato...

CN = IHO S-63 Scheme Administrator  
OU = International Hydrographic Bureau (IHB)  
O = International Hydrographic Organization (IHO)  
L = Monaco  
S = Unknown  
C = MC

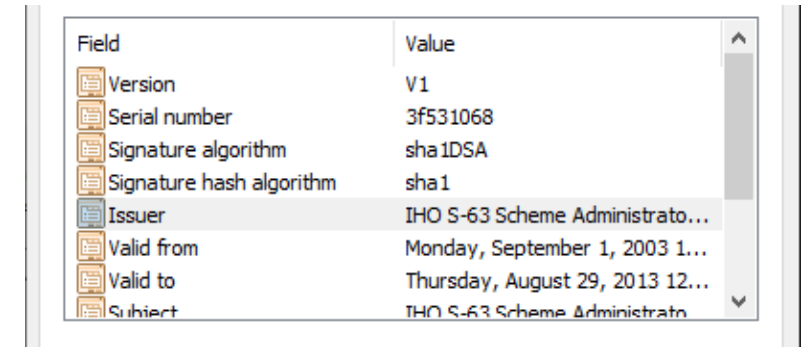


# Problem #3

- 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

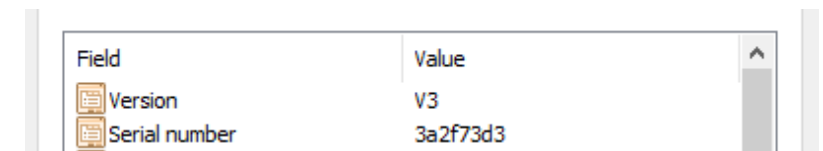
- **Issue:** Certificates of standard X509 have first version = X509v1
- **Expects:** Certificates of standard X509 third version = X509v3
- **Reason:** S 63 standard state that third version certificates X509v3 should be installed
- (5.4.2.4 The SA Digital Certificate (X509v3) Format)

**Actual:**



Field	Value
Version	V1
Serial number	3f531068
Signature algorithm	sha1DSA
Signature hash algorithm	sha1
Issuer	IHO S-63 Scheme Administrato...
Valid from	Monday, September 1, 2003 1...
Valid to	Thursday, August 29, 2013 12...
Subject	IHO S-63 Scheme Administrato...

**Expected:** IHO (like on the below picture)



Field	Value
Version	V3
Serial number	3a2f73d3