We observed that test data set which is part of standard have several issues.

Issue 1.

In the item «2.5.4 a) Install and validate the SA certificate and/or public key» is using file of certificate UKHO.CRT (from the test data set S-64_ENC_Encrypted_TDS/4 Authentication_Part1/Test 4a/UKHO.CRT). In the test case is checking that UKHO.CRT should be install into the system successfully and system should display warning ***SSE26*** - ***This ENC is not authenticated by the IHO acting as the Scheme Administrator".***
We found out that file of UKHO.CRT is incorrect and does not comply S-63 Standard.

How we understood that?

Based on items of standard S63 Edition 1.2.1 – March 2020 (*see attach. S 63_2020_Ed1.2.1_EN_Draft_Clean.pdf*):
- 5.2 Digital Certificates (SA Authentication)
- 5.4.2.4 The SA Digital Certificate (X509v3) Format
Certificate must be **root certificate** and should comply to standard **X509v3** (third version of X509)

If print info for UKHO.CRT using standard utility "openssl" (*see attach. UKHO-CRT-info.log*) then we can see in the section **X509v3 extensions**:

```
X509v3 extensions:
    X509v3 Basic Constraints: critical
        CA:FALSE, pathlen:0
```

What means CA:FALSE?
On the official web site (https://www.openssl.org/docs/manmaster/man5/x509v3_config.html) of utility "openssl" on the Section STANDARD EXTENSIONS / Basic Constraints we can see:

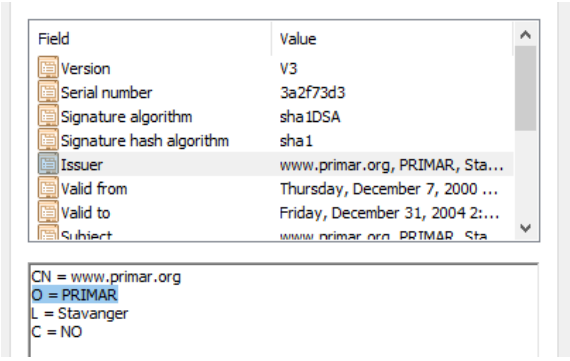
> A CA certificate **must** include the basicConstraints name with the **CA** parameter set to **TRUE**.
> An end-user certificate must either have CA:FALSE or omit the extension entirely.

It means that UKHO.CRT is not root certificate due to CA:FALSE –it is not comply to S63 – therefore we cannot install it using Legend.

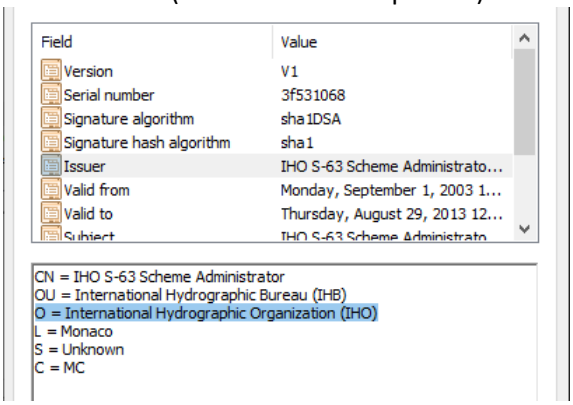
Looking for other Certificates of test data set of S64 we have found several more incorrect created certificates which do not comply to S63.

1. 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
   Must be: CA:TRUE
   Reason: Like described above – due to this reason the Certificates are not Root Certificates

2. S-64_ENC_Encrypted_TDS/4 Authentication_Part1/Test 4d/Expired/IHO.CRT
   Issue: The field "Issuer" contain record PRIMAR



Must be: IHO (like on the below picture)



Reason: Installation of Certificate with wrong field "Issuer" lead to warning SSE 26. This is **not expected** as per 2.5.4 d) of Standard S64.

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

   Must be: 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)