Proposal for amendments to S-63 for managing cyber security issues

ENCWG5 Online Meeting, 15-16 July 2020

Outline

- Background for new security requirement
- Current encoding of digital signatures in S-63
- Proposal extended S-63 signatures
- Description of available S-63 testdata where all files have a digital signature

Background

- S-63 and S-100 part 15 defines a Data Server role enabling a service provider to become a trusted member of the IHO data protection scheme
  - Has functionality to digitally sign files which can be authenticated using an IHO issued Data Server Certificate
  - Authenticates the file has been digitally signed by a member of the IHO Data Protection Scheme
- IMO and IEC require that *all files* in an exchange set must have a trusted digital signature to reduce ecyber security risks
  - ECDIS will not import unsigned ENC data and allow it to be used for safe navigation
- S-100 and S-100 part 15 standards have established mechanisms to support digital signing of all files in exchange set

Encoding of Signatures in S-57/S-63

- Use of encryption and digital signatures is optional
- Only ENC cells and update files are encrypted/signed
- Each ENC cell and update file have a separate signature file
  - Signature files encoded in CATALOG.031 file in CATD record
- Signature naming convention defined in S-63 para 5.3.2:
  - ENC file: CC[1-6]XXXXX.EEE (see S-57 Appendix B1)
  - Signature file: CC[I-N]XXXXX.EEE
- Example:
  - Update NO4ABCDE.001 has signature file NOLABCDE.001

Navigational Purpose	Signature Character
1. Overview	I
2. General	J
3. Coastal	K
4. Approaches	L
5. Harbour	M
6. Berthing	N

Example S-57/S-63 Signature File

PRIMAR®

```
// Signature part R:
7791 9CCA C248 B120 CCC9 7798 CB1A 9168 E0E0 39D4.
// Signature part S:
1CD0 84E5 8731 7FCF 7E97 509F 0515 B1AA ABC7 6BD6.
```

Data Server signature of ENC file

```
// Signature part R:
7AAF 45AF D759 7558 0D3F B52E AEDC 7C9F 7E77 BF4F.
// Signature part S:
18A9 D232 DF9D B01B 51D5 91D8 F71A A967 3D7A 9863.
```

SA (IHO) signature of Data Server Certificate

```
// BIG p
FCA6 82CE 8E12 CABA 26EF CCF7 110E 526D B078 B05E DECB CD1E B4A2 08F3
AE16 17AE 01F3 5B91 A47E 6DF6 3413 C5E1 2ED0 899B CD13 2ACD 50D9 9151
BDC4 3EE7 3759 2E17.
// BIG q
962E DDCC 369C BA8E BB26 0EE6 B6A1 26D9 346E 38C5.
// BIG g
6784 71B2 7A9C F44E E91A 49C5 147D B1A9 AAF2 44F0 5A43 4D64 8693 1D2D
1427 1B9E 3503 0B71 FD73 DA17 9069 B32E 2935 630E 1C20 6235 4D0D A20A
6C41 6E50 BE79 4CA4.
// BIG y
4645 6F86 5627 2ECE 4121 5354 D4EA AD75 1C62 71AA E80D 92DF EBB2 3212
3AAF 07AE E04E D252 58FF 3BCE 15E1 CDAA C7FC 7623 E9A6 5058 678C 8BB7
0419 265A 08D5 4786.
```

SA signed Data Server Certificate

Encoding of ENC signature files in CATALOG.031

Definition of ENC cell NO2A3620.000
and corresponding signature file NOJA3620.000

Definition of ENC update file NO2A3620.001
and corresponding signature file NOJA3620.001

Objectives S-63 signature proposal

- Introduce digital signatures on all files in S-57 exchange set compliant with S-63 to reduce the cyber risk during transit of data to the end-user
- Ensure proposal works on:
  - All OEM systems currently in use without any operational issues
  - Future OEM systems compliant with additional S-63 encoding

Proposal extended S-63 signatures

PRIMAR®

- ENC base cells and update files are digitally signed as before (NO changes)
- All other exchange set or service files
  - Digitally signed using the same algorithms as defined in S-63
  - Signatures will be encoded in S63_SIGNATURES.XML file in the INFO folder
- This method applies to:
  - CATALOG.031, README.TXT, PRODUCTS.TXT, MEDIA.TXT, SERIAL.ENC, STATUS.LST, PERMITS.TXT and any other service files

Structure S63_SIGNATURES.XML

```
<?xml version="1.0" encoding="utf-8"?>
<S63CombinedSignatureFile>
   <S63DataServers>
      <S63DataServer
         dataServerId=”ID”
         name=”Name identifying Data Server”
         R=”IHO signature of DS public key, see S-63 §5.4.2.6”
         S=”IHO signature of DS public key, see S-63 §5.4.2.6”
         p=”Data Server public key file, see S-63 §5.4.2.6”
         q=”Data Server public key file, see S-63 §5.4.2.6”
         g=”Data Server public key file, see S-63 §5.4.2.6”
         y=”Data Server public key, see S-63 §5.4.2.6”
         root=”IHO.CRT”>
      </S63DataServer>
   <S63FileSignatures>
      <S63FileSignature
      dataserverID=”ID”
      Path=”full path and file name”
      R=”Data Server digital signature of referenced file”
      S=”Data Server digital signature of referenced file”
   </S63FileSignature>
</S63CombinedSignatureFile>
```

Definition of all IHO Data Server Certificates used in Exchange Set

Definition of digital signature for each additional file in Exchange Set

Example S63_SIGNATURES.XML

```
<?xml version="1.0" encoding="utf-8"?>
<S63CombinedSignatureFile>
   <S63DataServers>
      <S63DataServer
         dataServerId=”PM” name=”PRIMAR”
R=”7AAF 45AF D759 7558 0D3F B52E AEDC 7C9F 7E77 BF4F”
S=”18A9 D232 DF9D B01B 51D5 91D8 F71A A967 3D7A 9863”
p=”FCA6 82CE 8E12 CABA 26EF CCF7 110E 526D B078 B05E DECB CD1E B4A2 08F3 AE16
17AE 01F3 5B91 A47E 6DF6 3413 C5E1 2ED0 899B CD13 2ACD 50D9 9151 BDC4 3EE7 3759
2E17”
q=”962E DDCC 369C BA8E BB26 0EE6 B6A1 26D9 346E 38C5”
g=”6784 71B2 7A9C F44E E91A 49C5 147D B1A9 AAF2 44F0 5A43 4D64 8693 1D2D 1427
1B9E 3503 0B71 FD73 DA17 9069 B32E 2935 630E 1C20 6235 4D0D A20A 6C41 6E50 BE79
4CA4”
y=”4645 6F86 5627 2ECE 4121 5354 D4EA AD75 1C62 71AA E80D 92DF EBB2 3212 3AAF
07AE E04E D252 58FF 3BCE 15E1 CDAA C7FC 7623 E9A6 5058 678C 8BB7 0419 265A 08D5
4786”
root=”IHO.CRT”>
      </S63DataServer>
   </S63DataServers>
   <S63FileSignatures>
      <S63FileSignature
         dataserverID=”PM”
         Path=”ENC_ROOT/CATALOG.031”
         R=” 5EA5 543D 826E F643 3DA5 B16D B4B0 52BA FF1D 4C8F”
         S=” 3B89 056C B37C BD07 2758 90C6 4526 EFEC E3CE 1790”
      </S63FileSignature>
   </S63FileSignatures>
</S63CombinedSignatureFile>
```

Discussion extended S-63 signatures

- Data Server Certificate(s) defined only once in first block of S63_SIGNATURES.XML file
  - Avoids repeating definition of Data Server Certificate for each file
- Not necessary to digitally sign S63_SIGNATURES.XML file since it is only a placeholder for file references and their signatures
  - OEM must always authenticate the included Data Server Certificates using IHO root key and all file signatures
  - Not possible for hacker to change or add files or signatures to S63_SIGNATURES.XML without being identified
- Data Server only needs S-63 Data Server Agreement with IHO (already signed to become a S-63 Data Server)
- Can be used with all existing ECDIS systems in use and all future systems developing support for extended signatures

Details of extended S-63 testdata

- All data digitally signed by PRIMAR and can be authenticated using the IHO issued PRIMAR Data Server Certificate (included with the data)
- Testdata contains the following files:
  - 1.ZIP: exchange set with cells, text and picture files
    - Additional signatures stored in S63_SIGNATURES.XML in INFO folder
  - 2.ZIP: exchange set with updates to one cell in 1.ZIP
    - Additional signatures stored in S63_SIGNATURES.XML in INFO folder
  - PERMITS.ZIP contains a permit file for the above above exchange sets and includes a permit signature file
  - Using same testdata as in S-64 test 2.1.1 and 2.2.2

Manufacturer info extended S-63 testdata

PRIMAR®

- Uses same manufacturer information as defined in S-64
  - Manufacturer ID: (M_ID) = 10 (or 3130 hexadecimal)
  - Manufacturer Key: (M_KEY) = 10121 (or 3130313231 hexadecimal)
  - Hardware ID: (HW_ID) = 12345 (or 3132333435 hexadecimal)
  - UserPermit = 66B5CBFDF7E4139D5B6086C23130