IHO S-63 DATA PROTECTION SCHEME

Proposal - Amended requirements for the definition and encoding of digital signatures for all files included in S-63 exchange set and service

1 Introduction

The IHO S-63 Standard was developed for encrypting, securing and compressing electronic navigational chart (ENC) data. It was first released in December 2002, and was based on the data distribution requirement, as they existed at that time.

It has recently been brought to the attention of the IHO that the scheme has possible shortcomings which could make it vulnerable to certain types of cyber security threat. Within every IHO S-63 encrypted exchange set there are a number of files that that carry no digital authentication signatures. The following files in an ENC exchange set are currently unsigned.

ENC Data: Auxiliary text and picture files .TXT & .TIF

Metadata Files:
CATALOG.031
README.TXT
PRODUCTS.TXT
MEDIA.TXT
SERIAL.ENC
STATUS.LST

Before the IHO decides to make any changes to the S-63 standard to resolve this shortcoming, it had been decided that an impact assessment, that includes all key stakeholders, should be conducted. The assessment will seek to understand the likelihood of an attack, its impact on the ECDIS and subsequent safety of the vessel. This must then be balanced against the time required to implement the necessary changes to the IHO standard, the cost to OEMs and the shipping industry. The impact assessment will also take account of expected release of S-101 exchange sets which will address this shortcoming, in 2024.

For OEMs to make an informed assessment of these issues and the effort required to update ECDIS to comply with a New Edition (NE) of S-63, the IHO has produced a fictious set of encrypted ENC test data that contains additional digital signatures.

This offers one possible solution to manage this problem. Feedback will be sought on the feasibility of the proposed solution and any issues it may raise with its implementation.

2 Objective of amended test data

The objective of the described proposal:

- Introduce digital signatures on all ENC files within an exchange set to reduce the cyber risk during transit to the end-user.
- Ensure the method can work on all existing OEM systems without any operational issues, and also that it is workable on any OEM system which has developed support for the additional S-63 digital signature encoding.

3 Test data Setup

The test data uses the same Manufacturer information as defined for the encrypted test data in IHO publication 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
- Digital Certificate: PRIMAR issued by IHO

3.1 Content of Test Data

The following cells are included in an exchange set;
GB4X0000
GB5X01NE
GB5X01NW
GB5X01SE
GB5X01SW
GB5X02SE

The cells have updates and supplementary text and picture files. A permit file will be provided along with an XML digital signature file.

4 Signature Method

The following method will be used to digitally sign all files included in an S-63 protected service provided by the data server.

- ENC base cells and update files:
  Digital signatures will be encoded in accordance with IHO S-63 Edition 1.2.0 chapter 5.3. In general the ENC file in the format CC**[1-6]**XXXXX.EEE will have a signature file CC**[I-N]**XXXXX.EEE located in the same directory as the source ENC file. This will not require any change to the current S-63 operation or functionality among Data Servers and OEMs.
- All other files included in the service:
  All other exchange set and service files will also be digitally signed. Each file will be digitally signed using the same algorithms as defined in S-63. A separate signature file S63_SIGNATURES.XML will be created containing the signature of each individual file included in the dataset exchange or service files. The signature file will be XML encoded. The signature file S63_SIGNATURES.XML will be located in the INFO folder on a hard media or supplied with the data for online deliveries. This method applies to CATALOG.031, README.TXT, PRODUCTS.TXT, MEDIA.TXT, SERIAL.ENC, STATUS.LST, PERMITS.TXT and any

other service files provided by the service provider. An XSD will be provided for XML validation purposes

The generic syntax for such a signature file is:

- The first block of data <S63DataServers> will contain a definition of all the Data Server Certificates being used in the exchange set. There will be one record for each Data Server. The intention is that the OEM can initially authenticate the data server certificates using the IHO public key. If successful, authentication, the OEM can extract the data server public key and use it whenever a file is to be authenticated.
- The second block of data <S63FileSignatures> will contain the digital signature for each file. There will be one record for each file included in the exchange set. The record will include a reference to the Data Server Certificate defined in the first block and identify which public key the OEM should use during file authentication.

A generic example:

```
<?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>
            <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=”ID”
            Path=”full path and file name”
            R=”Data Server digital signature of referenced file”
            S=”Data Server digital signature of referenced file”
      </S63FileSignature>
      <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>
```

4.1 Method discussion

- The proposed method is based on the same structure which will be implemented in the next edition of the IHO S-100 Part 15.

Example – from Part 15

```
</products>
<digitalSignature>
      <signedpublicKey id="primar"
rootKey="IHO">MIIBtjCCASsGByqGSM44BAEwggEeAoGBAMwvcLfFri7klqxaTwztsWCgcYqOh
NpKx7vIzstyiVM+xZlfgljKDToRQito0AIy9nkfXCOXA1QzuUhMNoLim8sloudLOeiDwjHq7fnm
/HNQVLNKG9XFxOSChBz8AaknPTPnSRuTv1JiTKzH17CAGhkCFzqf7kK+AexqttT05skhAhUApHD
c0AdnfLvcB6lQco/biZ7cv2UCgYBDWl36giFV2j4R2B7AxDmwwylcif7KiEeU9T+rrzQbQfIMCJ
eRLHVmNe0uO/L9YStBWNd+7vUIHQVzRNRmcODHlQTbojm8FSofNyOKc3LbQraAlMG/dcrDX7Xaf
gFpdeCcyNyntD+7nd076zATYec5Ad4RJeo1Bq/UphJPYBSpNgOBhAACgYAIb5BNjP4YJOw/y7dc
US2k7aLt3YaWEM8sIyhOAGo4Z8bpzdDRkj5NYSYSzqKzHBTVRxPna4YKf7XvTQwflhWDDCo+yCu
YirLFsmMJv5Mp8wL8+MXZNr4IAlk/xgTBCZfZPdbAaGpoQ4nmgt0tQyJBxck+M2jUjGbQ2VCECI
sNQQ==
</signedpublicKey>
      <signature>
            <R>28F549549614ED4896BECBB056BE0F36ECA172EC</R>
            <S>399A5F5FC5B4DC52F1B750233F85AE3849227603</S>
      </signature>
</digitalSignature>
</permit>
```

- The permit file will have a S63_SIGNATURES.XML since it can be distributed without any exchange set
- By defining the Data Server Certificates initially with an ID in the first block, it will not be necessary to include the R, S, p, q, g and Y parameters every time a file signature is defined. The OEM can just look up the Data Server ID and use their public key.
- The signature file S63_SIGNATURES.XML will not have a signature itself, and it will not be required for cyber security reasons. Since it will only be a placeholder for file references and their digital signatures, the OEM application shall always:
  1. Authenticate all Data Server Certificates against the IHO root key. Any Data Server Certificates which fail authentication shall NOT be used.
  2. Authenticate the applicable ENC or service files by using the proper Data Server Public Key (authenticated in step 1 above) and using the supplied R/S signature elements found in the S63_SIGNATURES.XML.
- It will not be possible for any hacker to introduce any new files or change any of the existing files in the exchange set or service files since the authentication will fail because:
  1. They do not have a Data Server Certificate which can be authenticated using the IHO protection scheme public key;
  2. They will not be able to impersonate a Data Server so the individual file authentication will fail;

3. It does not matter if they try to add additional file records into the collated signature file because they are either not referenced by the ENC data (text or picture files) or the authentication will fail because they try to use a non-authenticated Data Server Certificate; and
4. The only organization which can introduce a cyber risk in this setup is a registered Data Server with improper operational procedures, or someone who has got hold of a Data Server private key.