Paper for consideration by S-100WG

Data integrity and the relationship of S-63 ed2.0 to S-100/S-101

Submitted by:	Jonathan Pritchard [Chair DPSWG]
Executive Summary:	A proposal for a mechanism to deal with data integrity within S-100 and its product specifications. Recommendations are made for additions to metadata specifications and how IHO S-63 supports the development of data integrity mechanisms in data products.
Related Documents:	None.
Related Projects:	None.

Introduction and Background.

Currently IHO S-63 provides the following facilities for use within S-57 ENCs.

1. Data Compression (via the zip format)
2. Data Encryption via the Blowfish algorithm and the production of permits
3. Data Authentication via DSA format digital signatures

S-63 also provides a number of facilities to assist the import of ENC data into ECDIS (e.g. the products.txt file). The S-63 format is implemented by ECDIS manufacturers, entities distributing ENC data commercially, some hydrographic offices and third party software providers. The use of the S-63 format for protection/authentication of data is performed within the IHOs data protection scheme, the details of which are also documented within the current edition of IHO S-63. It is worth noting that S-57 itself provides no facilities for data encryption but it does utilise the CRC32 algorithm for data integrity. This mechanism provides a basic check of data integrity prior to a cell being imported into a receiving system. The main idea of S-63 was that it could be applied to an unencrypted exchange set providing its facilities in a layered fashion. In recent years the implementation of S-63 has spread and there is a growing interest in implementing its component parts without implementing the entire standard, e.g. to allow the production of digital signatures without the need for an implementation of data encryption protocols.

Analysis/Discussion

There is a continuing need within the IHO community to continue to provide these facilities within the S-100 and S-101 regime and to provide a framework standard which will allow:

1. The provision of data protection, compression and authentication to data product specifications
2. The ability for modular application so that encryption and authentication are not inter-dependent.
3. The ability to tailor protocols and implementations for different product specifications.

IHO DPSWG has met on this subject several times and a proposed structure has been arrived at through discussions with hydrographic offices, RENCs and ECDIS manufacturers. The main principles within the new edition of the standard are:

1. To provide an overall requirement within S-100 for some form of data integrity mechanism without prescribing its implementation.
2. To provide a normative data authentication mechanism and supporting identity management structure[1] (i.e. the IHO data protection scheme) specifically for use with S-101 ENCs.
3. To provide a standalone data protection and encryption mechanism for implementers, again, within a supporting structure of the IHO data protection scheme.

It is therefore proposed that S-100 and S-101 reflect these principles and refer to S-63 for implementation details where needed.

Structure of the new edition of S-63.

In order to address these requirements the new edition of s-63 (currently being drafted by the DPSWG) has the following structure.

- Part A(i) – Encryption and copy protection mechanisms. Includes specifications for permits and OEMs. Uses Blowfish encryption and permit structure. Also includes compression via Zip prior to encryption. This is aimed at S-101 content but is usable by other, similar product specifications.
- Part A(ii) – "Service elements". Defines products.xml and high level exchange set structure.
- Part B – Strong integrity - Digital Signatures. Depends on Part C for some content. Defines a scheme usable by multiple product specifications if need be but primarily for S-101. Only has single algorithm so won't be updated in the future. Again, this is designed for use with S-101 product specifications but should be usable by other data products similarly structured.
- Part C – Operation and management of the IHO Data Protection Scheme and its members. Definition of "identity" within the data protection scheme, keys, signing, root certificates + procedures for implementation. Refers to Part B for format descriptions. This applies across the board to any product specification requiring the application and verification of digital signatures.

The algorithms and structure of the data protection scheme remain intact. The concept is still that of allowing access to encrypted data and digital signing of individual datasets within an identity assurance scheme operated by the IHB.

The main proposals of this paper (i.e how S-63 edition 2.0 interfaces with S-100, S-101 and other S-100 product specifications is as follows:

1. S-100 contains a generic requirement for a data integrity measure and a recommendation for ECDIS based product specifications to contain a strong integrity measure ideally S-63's digital signature mechanism (implemented within the IHOs data protection scheme defined

[1] Essentially a digital signature is a checksum which can be authenticated against a known identity. In order to assure identity a trusted party must verify the data issuer. Currently the IHO data protection scheme provides this function for scheme members. In short digital signatures require an identity management scheme.

by s-63 ed2.0 part C). S-100 also states that data encryption is optional in product specifications.

2. S-101 mandates use of digital signatures as their data integrity measure. S-63 ed2 Part B provides a normative reference for construction of these digital signatures.
3. S-101 specifies an optional data protection mechanism for encrypting data and producing permits to unlock data. This can be applied independently of digital signatures. If data encryption has been implemented then "service" elements of S-63 should also be constructed although these are external to S-101 data and metadata.

File and Formats.

One of the difficulties of implementing S-63 is the text based formatting of the various keys, signatures and other auxiliary files specified as part of the standard. S-63 edition 2.0 is proposing a simpler format for the parts of the standard to be included in S-101, specifically the public keys and digital signatures used for the data authentication. The proposal is to use base64 encoding to hold the complex sequence of bytes representing digital signatures so that instead of the S-63 edition 1.* representation of :

```
// 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
67E7 F248 E02B E0C7 ABFF 6FAD 8C84 0367
01E0 3069 D24D EF62 1A53 90D7 917B 54F8
C6DE 3F55 2316 A4B0 3C7D E373 8F34 046A
4561 4AB6 F164 41F9 EF35 AF78 43CE 6FF7.
```

A far simpler XML enclosed text string as follows is used:

```
<publicKey>/KaCzo4Syrom78z3EQ5SbbB4sF7ey80etKII864WF64B81uRpH5t9jQTx
eEu0ImbzRMqzVDZkVG9xD7nN1kuFwli7dzDacuo67Jg7mtqEm2TRuOMU=Z4Rxsnqc9E7
pGknFFH2xqaryRPBaQ01khpMdLRQnG541Awtx/XPaF5Bpsy4pNWMOHCBiNU0NogpsQW5
QvnlMpA</publicKey>
```

This format of xml enclosed base64 data ensures a much more reliable transfer of the content of the signatures and the bytes making up each of the elements. This also means that implementers do not need to worry about the exact syntactical formats of the various files in S-101.

Recommendations.

1. [S-100] That a generic requirement for a data integrity measure (previously "checksum") in all product specifications is added to S-100

2. [S-100] ECDIS specifications should use the data integrity measure and supporting structures documented in S-63 ed2.0 Parts B and C. Any product specification wishing to implement digital signatures should use the Part C identity management scheme (although they may wish to define different protocols, algorithms etc.. replacing Part B).
3. [S-100] Feature and Portrayal catalogues for S-101 datasets should be digitally signed by the scheme administrator prior to distribution as a security measure and to prevent corruption of end user systems.
4. [S-101] The implementation of the data integrity measure is S-63's digital signature mechanism as documented in S-63 part B. The IHO data protection scheme documented in part C of S-63 provides the authenticated identity required by the digital signatures.
5. [S-101] that a "publicKey" and "digitalSignature" XML element is added to the S-101 catalogue metadata specification to allow inclusion of these elements for S-101 exchange sets.
6. [S-101] data protection (=encryption) is optional. If implemented it should be done according to the standard documented in S-63 part A. an "isEncrypted" flags should be included in the catalogue metadata as well to tag datasets which are encrypted.
7. DPSWG drafts updates to IHO S-100 and IHO S-101 reflecting these modifications.