TSMAD 26 11.9A

Paper for Consideration by TSMAD 26

S-100 - Data Integrity Measures

Submitted by:	DPSWG
Executive Summary:	This paper requests TSMAD to insert a wider variety of data integrity measures into S-100
Related Documents:	
Related Projects:	1. DPSWG Work item – Development of new edition of S-63.

Introduction / Background

1. In February 2013 DPSWG9 was held in Monaco. This meeting reviewed current progress against a new version of S-63 which can be used in conjunction with future S-100 based datasets, in particular ENC data.

2. The meeting acknowledged that a considerable proportion of the existing S-63 standard is derived from the old Primar Security Scheme and replicates content and metadata within the S-57 standard. In particular, the mechanism of digital signatures represent a duplicate method of data integrty measure within the exchange set.

3. It was also noted that different entities within the data supply chain have different requirements of IHO standards and, whilst S-63 provides data compression, encryption and authentication/integrity, IHO member states may only have an interest in data integrity and may choose not to encrypt (or indeed compress) their ENC data for distribution.

4. It was therefore recommended by DPSWG that a more logical approach to the issue of data integrity would be to request TSMAD to add non-mandatory extensions to S-100 to allow a wider range of data integrity mechanisms to be embedded into future S-10x products and to draft an instance of those data integrity measures within S-101 for use within ENC leaving the future S-63 standard to concentrate on wider distribution methodologies and tools.

Analysis/Discussion

5. IHO S-57 uses a 32 bit cyclic redundnacy check CRC-32 value to provide data integrity. After a dataset is written to external media a CRC-32 value is computed and inserted into the catalogue entry (CATD) for the cell. This provides the only means of checking whether an ENC cell has been altered in transit to an end user – once the dataset is extracted the CRC-32 value can be re-computed and checked against the CATALOG.031 CATD entry.

6. Although this system provides a level of data integrity it is open to both error and abuse. CRC-32 values are relatively easy to fake and there is plenty literature on the subject. A stronger mechanism is to encrypt the CRC value using a public key cryptographic algorithm such as RSA. This strengthens the data integrity check and gives a stronger data integrity method. Currently IHO S-63 provides a digital signature facility independently of S-57s CRC-32 value. S-63s algorithm is based on the US Digital Signature Algorithm (DSA).

7. The requirement for data integrity still exists and both originating hydrographic offices and ECDIS end users have an implicit need to know that data has not been altered in transit. Providing a single data ingrity mechanism is more intuitive to the user and can meet a variety of member state requirements for labelling their data. There is a clear distinction made between data integrity and data “security” though.

S-63s facilities for encryption and compression are generally used by ENC service providers as the framework for a distribution system.

8. In order to reduce the scope and duplication of a new edition of S-63 the following additions are proposed to TSMAD areas of interest:

a. A general “data integrity” measure to be included in S-100s concept of dataset. This will be specific to a particular encoding of a dataset and will have a general concept of “algorithm” – i.e S-100 itself does not specify a particular algorithm to be used as the data integrity measure. It should be discussed whether a data integrity mechanism is mandated regardless of the algorithm. Certainly it would seem sensible that datasets always contain some kind of integrity check . The addition in S-100 would leave the implementation details up to the individual product specification.

b. A data integrity measure for S-101 which embeds CRC-32 and DSA as potential data integrity measures.

9. DPSWG is happy to draft any necessary documentation to support these changes within S-100/S-101 and

Conclusion

Action Required of TSMAD

-