S-100TSM7-5.15

Paper for Consideration by S-100TSM7

S-100 part 15 clarification and improvements

Submitted by:	ECC
Executive Summary:	This document covers a range of improvements to the standard arising from our implementation of the S-100 part 15 data protection
Related Documents:	
Related Projects:	

Introduction / Background

Electronic Chart Centre (ECC) has started to develop support for data protection in accordance with S-100 Part 15 which was published in December 2018.

We have in our development identified a range of issues where a clarification and possibly testdata can be improve the readability and understanding of the S-100 data protection scheme.

Analysis

1. S-100 part 15 uses XML for the exchange of information. The IHO standardization working groups should ideally include a XML Schema Definition file (.XSD) to formally describe all the data protection elements defined in S-100 part 15. (This also applies to all S-1xx standards). The Schema Definition files should have a version numbering in the schema URL corresponding the same edition of the standard. This will support automatic verification of file structure and content.

2. When a XML file is included in the exchange set, and used as an example in the documentation or as test data, they should always include a proper XML header. The header can also include a reference to where the schema is defined. This particularly applies to the exchange of permit files issued by a Data Server.

3. S-100 part 15, nor any of the S-1xx product specifications, specify how the exchange set catalogue file will be digitally signed. The signature of the catalogue file should not be included in the catalogue file itself, it is recommended to create a separate signature file in the same folder as the catalogue file itself. The signature file will re-use the full name of the catalogue file, but will have ".signature" appended. The content of the catalogue signature file will be the Data Server Certificate and the catalogue file digital signature. This will enable the recipient system to authenticate the Data Server Certificate and certificate validity, and extract the P, Q, G and Y parameters from the Data Server Certificate and use it to authenticate the signature of the catalogue file. A possible encoding of such a signature file can be:

```
<?xml version=”1.0” encoding=”utf-8”?>
<S100XC:digitalSignatureValue xmlns:S100XC=”http://www.iho.int/s100/xc”>
<S100XC:digitalCertificate>
-----BEGIN CERTIFICATE-----
MIIFjDCCBUqgAwIBAgIFAK2CkKMwCwYJYIZIAWUDBAMCMHExGzAZBgkqhkiG9w0B
CQEWDHRlc3RAdGVzdC5ubzENMAsGA1UEAwwEdGVzdDENMAsGA1UECwwEdGVzdDEW
……… (deliberately removed to reduce size)
NX7GTM+Oz6EHwwIUNhHAon/ruVlRV/5/wLyNwO672t4=
-----END CERTIFICATE-----
</S100XC:digitalCertificate>
<S100XC:digitalSignature>MCwCFFq84AtsRA9OlnRsi0Vt896UC5E+AhQUw4TCr88tYncUx7
w6zunLJb4fCw==
</S100XC:digitalSignature>
</S100XC:digitalSignatureValue>
```

This is the same approach used by the IHO S-100 Scheme Administrator application which has functionality to add a digital signature to files issued by IHO; e.g. the S-101 feature catalogue. Since it was assumed all files in the feature catalogue will be zipped before publication, it was decided to store the signature in a separate. This will ensure the recipient can use the files directly in a word processor, PDF reader or unzipping software without the need for dedicated software to split the certificate/signature element from the original file. It will still be possible to authenticate the signature associated with the feature catalogue if sent to a vessel.

There is also another option to add the certificate/signature element at the end of the catalogue file to encode the catalogue file signature, see more information in item 4 below.

4. This is related to item 3 and how the signature element for a permit file is to be provided and encoded. S-100 part 15 Chapter 7.4.5 includes a permit example where the signature is appended to the end. To ensure a proper authentication of the signature must the permit file include a copy of the Data Server Certificate and the signature of the permit file (excluding the certificate/signature element). If the certificate and signature will be included in the permit file and not encoded as a separate file, it is important to include a precise definition in S-100 part 15 of which parts of the permit file should be used for authentication; especially if carriage returns/line feeds between the permit and certificate/signature definition shall be included in the file authentication.

5. S-100 part 15 Chapter 7.4.5 permit example: The <permit> element is used twice for two different purposes. It is suggested to rename one of the <permit> elements; e.g. rename the individual permit to <datasetPermit>

6. S-100 part 15 Chapter 7.4.5 permit example: A product element is used to encode or group together all the permits provided for a specific product, e.g. S-101 permits. The current naming convention is to include the product name in the beginning of a dataset name; e.g. 101N100B11TESTS.000 for a S-101 file. If this naming convention will be applied for all S-100 based product specifications, there is not a need for a separate <product> element in the permit file since it can be deduced from the three first characters of the file name. It requires however that all S-1xx based product specifications adheres to the same dataset naming convention.

7. S-100 part 15 Chapter 7.4.5 permit example: Filename with a suffix does not make sense for S-101 products because the permit applies to the base dataset and all updates issued to the current edition of the dataset. The update files to a base dataset will be have a suffix with sequential numbers. The naming convention does however meet the use of the element <filename> defined in DataSetDiscoveryMetadata.

8. S-100 part 15 Chapter 7.4.5 permit example: S-100 refers to ISO8601 for the definition of date formats. Many different dat formats are defined in ISO8601, including the possibility to use partial date definitions. "2019-05-14T09:22:46Z", "2019-05-14" and "20190514" are all valid date formats in accordance with ISO8601, but the first two are more commonly used. Is there a need to provide a more precise definition of a date format to be used in a permit file?

9. S-100 part 15 should be updated with appropriate worked examples and possibly some testdata which can be used by developers. ECC and PRIMAR can contribute to make testdata and worked examples available for developers as soon as we have obtained a S-100 Data Server Certificate.

Action Required of S-100TSM7

The S-100TSM7 is invited to:

- Discuss the proposals within this paper and decide whether they could be forwarded to S100WG5 for further consideration and approval