S-100WG3-9.3.1

Paper for Consideration by the S-100WG

Cyber security and Authentication issues

Submitted by:	Hannu Peiponen / IEC TC80 Chair
Executive Summary:	This paper informs S-100WG about coming absolute requirement to provide possibility to authenticate all data files.
Related Documents:	N/A.
Related Projects:	Development of S-100, Development of S-101, Development of S-10X product specifications

Introduction / Background

1. IHO has been recognized by IMO as being the governing body for providing nautical charts and publications, and to coordinate provision of Maritime Safety Information (MSI). Some of the related IHO activities are under HSSC (for example S-100WG, NIPWG, etc.) and some under IRCC (for example WWNWS-SC). Common for all activities is drafting of S-100 based Product Specifications.

2. IHO have had for long time a plan to include S-63 style cyber security into the S-100 baseline. Initial idea was 2nd edition of S-63 to handle S-100 based services. More recent idea has been to include principles of S-63 as a part in the S-100 baseline itself. Unfortunately, I assume due to lack of resources, so far very little has been achieved.

3. IMO has set generic guidelines to manage maritime cyber risk, see

- IMO MSC-FAL.1 Circ.3, Guidelines On Maritime Cyber Risk Management, 2017

4. IMO MSC-98, Jun 2017, published an IMO resolution MSC.428(98) which state that cyber risk is one of the issues to be addressed by ISM-code and the periodical audit of vessels for ISM-code shall include audit of management of cyber risk from 1st Jan 2021.

4. Response of industry has been creation of numerous private rules related to the IMO rules, for example

- BIMCO et.al., The Guidelines on Cyber Security Onboard Ships, 2017
- DNV-GL, Class Program DNVGL-CP-0231, Jan 2018
  This Class Program reference existing standard such as IEC 61162-460, which require authentication of data files and executables

5. IEC TC80 has also reacted by initiating drafting a new standard IEC 63154 Cyber security about what kind of mitigation against cyber risk the equipment onboard shall provide. Target of the new standard is to establish international consensus on the minimum technical level of mitigation against cyber risk. The timeline of this new standard is:

- Drafting by the workgroup until 1st quarter of 2020
- IEC approval process consisting of CDV and FDIS comments & votings from summer 2020 to the publishing planned for 2nd quarter of 2021

6. The current draft of the new standard IEC 63154 is based on the principle that all data files and executables should be authenticated for their source and integrity before use by the IEC 63154 compliant equipment (see IEC 80/883/CD). For IHO this means a need to provide authentication method of all data products from HOs to vessels regulated by SOLAS.

Analysis/Discussion

7. I recently attended the NIPWG-5 meeting (Mar 2018). The meeting had a lively debate around delivery of the Nautical Publications, especially as S-122 and S-123 has been completed to be ready for approval by HSSC-10, May 2018. This debate really highlighted the fact that the S-100 baseline is not yet ready to support anything else than the object modelling of a digital product.

8. There are obviously many open issues around service and delivery of S-100 based digital products. This paper address only cyber security part of these open issues.

9. The need for providing support for cyber security is so generic that the S-100 baseline should provide the solution instead of individual S-10X Product Specifications establishing their own regimes.

10. For the current S-57 ENC charts the S-63 has been a voluntary option. This optional nature of providing cyber security does not fit anymore the reality for digital nautical products intended for IMO SOLAS regulated vessels.

11. This is not the first paper related to cyber security and submitted by me to the S-100WG. For the previous S-100WG2 meeting I submitted paper "S-100WG2-10.18_Cyber_Security_and_Service_Issues". The analysis/discussion, conclusions and recommendations of that paper are still valid. The basic principle of S-63 to use the private-public key pair to facilitate creation of signatures and authentication of signatures is valid. Also, the proposal to facilitate more than one private-public key pair to overcome extension from just S-57 ENC chart service to multitude of many digital services by different domains is still valid.

12. This time there is one new observation to note for the development of the cyber security for S-100 based products. Namely the fact that the provided signatures shall cover all data files of the service. This observation rises from the fact that in the existing S-63 ed 1.2.0 for S-57 ENC charts only the ENC charts and their update files (i.e. .000, .001, .002, etc.) are protected by the signature, while auxiliary files (.txt, .tif), up-to-date information file (products.txt) and service related files (catalog.031, readme.txt, serial.enc, media.txt, status.lst) are not protected by a signature.

13. The up-to-date information file, auxiliary files and service related files offer numerous ways how a hacker could cause serious issues for a vessel. For example, up-to-date information file could cause removal of ENC charts from onboard navigation equipment, use of content of auxiliary files could cause serious mistakes in route planning, etc.

14. In S-100 terminology '*ENC charts and updates*' are '*datasets*', '*auxiliary files*' are '*support files*' and '*service related files*' are '*exchange set catalogues*' and '*exchange sets*'. Additional element not available in S-57 are machine-readable feature, portrayal, interoperability, etc, items named '*catalogue*'.

15. Review of the S-100 Ed 3.0.0 Part 4a, Appendix 4a-D for Exchange catalogues shows that S-100 has addressed quite many issues related to cyber security, but many details are still open

- Most of the metadata include 'digitalSignatureReference' (i.e. what is the method of calculation of digital signature) and 'digitalSignatureValue'
    - Dataset, Support file and Catalogue include these (better than current edition of S-63 which includes digital signature only for Dataset equivalent part)
    - It is looking like that the infrastructure level, for example, 'exchange set catalogue' and 'exchange set' miss digital signatures (i.e. like Products.txt, Catalog.031, etc. miss digital signature in current edition of S-63)
- Only S100_DatasetDiscoveryMetadata include a boolean flag 'digitalSignature' to inform, if the digital signature is available or not for a dataset file. All other uses of 'digitalSignatureReference' and 'digitalSignatureValue' are without this boolean flag.
    - Is this a mistake ? Should all have the boolean flag (i.e. signature being option for every component) or Should all be without boolean flag (i.e. signature being mandatory for every component)
    - Is this intentional, for example, that digital signature is mandatory for everything else than dataset files (i.e. ENC charts and updates are not protected while support files are always protected) ?
- 'digitalSignatureReference' is defined as 'Specifies the algorithm used to compute digitalSignatureValue'
    - But the S-100 ed 3.0.0 has no description of calculation methods acceptable for this

16. Review of the S-100 Ed 3.0.0 Part 11 for Product specifications shows that clause 11-16 specify

- '*Product specification may require use of digital signature*'
    - This acceptable as SOLAS class use requires and other use cases may not require
    - However there should be more strong guidance that digital signature is mandatory if the target of the product specification is SOLAS class vessels

- ‘*Where included, the details of signature method shall either reference to the IHO S-63 or be described in the product specification itself*’
    - Paragraph 15 of this report informed reader that there is no clear specification for ‘digitalSignatureReference’. The above wording tells that this ‘digitalSignatureReference’ should be either IHO S-63 or described by the individual product specification
    - IHO S-63 is a good alternative, but some details are missing
        - What is the exact text string used for IHO S-63 ? Perhaps ‘IHO S-63’ or ?
        - Description of how to apply IHO S-63 ?
            - Just calculate digital signature using IHO private key and then store the result in ‘digitalSignatureValue’ of metadata ? Or ?
            - Any description of use of the public key ? Or just follow the principle of S-63 when applied to an ECDIS compliant with S-57 ENC charts ?
        - In reality the usage scope of S-100 is much larger than original usage scope of S-63 intended for S-57 ENC charts and updates. Is it practical that all producers of any S-100 compliant data will apply for access to the private key of IHO ? Would it be more realistic to use the principle of S-63, but allow use of multiple pair of private-public keys (for example HOs use the original IHO private key, IALA use their own, IEC use their own, etc.)
            - To facilitate use of multiple private-public key pair requires that a description of this is included into S-100 itself
    - The other alternative is described by the individual product specification. Today this alternative is not looking realistic for SOLAS class vessels. This paper focus on SOLAS class use and is therefore neutral for leaving the door open for other use cases.

17. A good reminder of how bad the things could grow is what has happened for provision of digitalized ship reporting (IMO FAL reports). This process established a concept of “single window” meaning that a single copy of the ship reports per a port call should be used by all shore-based stakeholders (port authority, VTS, customs, police, immigration, etc.). The concept missed harmonization of the “single windows” and the result is that in best cases a “single window” was applicable for a single full country and in worst case a “single window” was applicable only for a single port in a country. Result of this “chaos” has been increase of burden for onboard crew and more expensive to run for the ship owners. The result is therefore totally opposite to the target of the IMO e-Navigation. (Keynote speech of Niels Smedegaard, CEO and President of shipowner DFDS, e-Navigation Underway 2018)

Conclusions

18. Provision of the cyber security is a matter of urgency. The next full edition 4.0.0 of S-100 should include a section on cyber security and should provide more guidance to those developing S-10X based product specifications.

Recommendations

19. Recommendation is to agree that addressing of cyber security shall be one of the targets of the next full edition 4.0.0 of S-100.

Justification and Impacts

20. We have all seen how difficult it is within IMO to overrule “grandfather” principle for already installed equipment. This means that the solution must be fit-for-the-purpose and complete from the begin.

Action Required of S-100WG

The S-100WG is invited to:

a) note the issues presented in this paper

b) consider what actions are needed to facilitate prompt drafting of the details of the cyber security into the next full edition 4.0.0 of S-100 baseline.