Paper for Consideration by TSMAD28

Cyber security and Service issues

Submitted by:	Hannu Peiponen / Furuno Finland
Executive Summary:	This is a discussion paper about how Cyber security and Service issues could be managed within S-100.
Related Documents:	N/A.
Related Projects:	Development of S-100, Development of S-101, Development of S-10X product specifications

Introduction / Background

1. IMO has selected IHO S-100 as baseline for e-Navigation related services. This decision will automatically lead to extensive conversion from paper based services to electronic S-10X services based on S-100.

2. The writer attended in January 2014 e-Navigation Underway conference at end of which there was a panel discussion. Industry was very worried about the cyber security of the future S-100 based services.

3. Cyber security can be understood to include integrity and authentication. In practice these means, is the content of the information as published by the origin instead of being tampered by hackers/criminals and is the origin as assumed or from hackers/criminals.

4. Service can be understood to answer is my information up-to-date.

Analysis/Discussion

5. Today the new S-10X services are still under development, but tomorrow is soon and the new S-10X services should from begin include cyber security and service aspects.

6. In the future the S-57 ENC charts will be replaced by S-101 ENC charts. Today there is practical solution for the cyber security and service aspects of S-57 ENC charts. The solution is named S-63. We can learn lessons from the history of the S-57 and S-63:

6.1 The S-63 is a voluntary add-on. This means that it is possible to bypass providing cyber security and service aspects. In practice there are many IHO member states which do not use S-63 although majority of the data from member states is available being compatible with the S-63.

6.2 There is one obvious reason for the resistance to S-63. The S-63 was initially promoted as a solution for piracy protection purposes, providing permits, licenses, encryption, selective available, etc. This was not acceptable for the member states who planned to provide free of charge S-57 ENC chart service.

6.3 The S-63 includes in the specification also non-encrypted option, use of which would allow cyber security and service without the piracy protection provided by encryption, permits, licenses, etc.. But this non-encrypted detail is well hidden into the text. Further IHO newer created a test data set to test use of the non-encrypted version. The encrypted version is supported extensively by test data and test instructions included into the S-64.

6.4 Someone could claim that the S-57 ENC charts without the S-63 include a CRC checksum in the Catalog.031 file for the integrity check. It is true that a CRC checksum could be used for the integrity check, but the CRC alone is too simple to hack (i.e. it can be used to identify unintended data transfer errors, but it is not strong enough against any intended cyber security attack) and the S-57 lack any method to protect the content of the CRC (i.e. an intended hacker/criminal can easily replace both the data content and the CRC).

7. In the S-63 the cyber security is taken care by the signature method. Each protected file has its own small signature file, which contain a signature calculated over the protected data content using private key only known by the data origin. The data origin publish a public key which is used together with the signature file both to authenticate the data origin and to check the integrity of the data content. This private-public key method is still state of the art for the cyber security purpose.

8. In the S-63 the service aspect for up-to-dateness of the data is handled by a file called products.txt. This file contains up-to-date information for each individual S-57 ENC chart available from the service. This information

enables an ECDIS to support the up-to-date awareness by providing standardized indications (for example SSE27) and by providing standardized up-to-date reports.

9. The S-63 contain in addition to details referenced in 7 and 8 a lot of specification details related to piracy protection, selective availability, etc.., but these details are not topic of this paper.

10. IHO has separate workgroup called DPSWG to maintain S-63. This workgroup include experts in cyber security, service, piracy protection and selective availability. The write is a member of DPSWG. However if we let the history to repeat itself then the cyber security and service aspects will live their own life outside the S-100 as they live outside the S-57. This is not good. The cyber security and service aspects should be included into the S-100 baseline as mandatory to implement for every S-10X product layer. The piracy protection and selective availability could be left for DPSWG to develop appropriate solution(s) for the S-10X based product layers.

Conclusions

11. The work for S-100 is off course not yet completed. This paper acts as a reminder of the work ahead.

12. The target of this paper is not to be a show stopper. We can also think that the next edition of S-100 includes a subset of the items needed and that there will be a timetabled next next edition to address the remaining. Important is that the cyber security and service aspect of the this paper have a solution before IHO announce that the S-100 is now fully tested and ready to play the big role as enabler of the e-Navigation.

Recommendations

13. The issues detected by this paper should be studied and, if needed, appropriate drafting processes should be initiated.

Justification and Impacts

14. 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 from initial full publishing..

15. If we fail to provide cyber security and service aspect from the beginning there will be later a need to provide software upgrades to address cyber security and service. Further this may lead to such situation that each S-10X product layer has its own solution for the cyber security and service aspects. This will create the problem as described in 14.

Action Required of TSMAD and/or DIPWG

The TDMAD and/or DIPWG are invited to:

a) note the issues presented in this paper
b) note that next next editions may be needed before the S-100 concept is ready to serve the purpose
c) consider to define what is task of TSMAD and what is task of DPSWG