S-100WG2-10.18

Paper for Consideration by the S-100WG

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

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.

Concern about cyber security and service has been expressed at several e-Navigation Underway conference and it has been agreed that this should be an issue to consider for future S-100 based products and services.

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.

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

Analysis/Discussion

Although S-10X services are still under development, it is proposed that all Project Teams should consider cyber security and service aspects from the beginning of their work.

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:

> 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.
>
> 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.
>
> 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. Furthermore, the IHO never 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.
>
> 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 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 lacks 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).

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 originator. 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.

In the S-63 the service aspect for up-to-datedness 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.

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

At the 8th DPSWG meeting it was decided to disband the Data Protection Scheme Working Group (DPSWG) which was responsible for the S-63 Security Scheme, and to split its functions between the S-100WG and the ENCWG. The continued maintenance of the existing scheme will fall under the ENCWG, and new development falls under the S-100WG. This work should include issues relating to cyber security, service, piracy protection and selective availability. It is proposed that cyber security and service aspects should be included into the S-100 baseline as mandatory to implement for every S-10X product layer. Where appropriate the piracy protection and selective availability should be developed by the relevant WG or PT for the S-10X based products.

The S-100 edition 3.0.0, currently waiting official publishing, includes first step toward providing solution for cyber security part. Namely the checksum in ed 2.0.0 has been changed as signature to be the placeholder for the signature to be used for authentication of the source and content. Although this is a step in correct direction, it is not yet the full solution. The main remaining for cyber security is to define the technical method of calculating the signature and defining the management procedures of the associated pre-shared private and public keys. Furthermore it should be considered whether one single private-public pair of keys is enough or should there be provisions for multiple keys, for example one pair of keys per domain owner for the S-100 registry.

It should be noted that although there has been a little bit of progress for the cyber security part, the service part (i.e. to know if my data is up-to-date), is still not yet started.

Conclusions

The next S-100 full edition 4.0.0 should include a section on cyber security and service aspect and should provide guidance to those developing S-10X based product specifications. This work should also take into consideration requirements for e-Navigation development activities.

Recommendations

The meeting is invited to discuss the issues presented in this paper, keeping in mind the legacy S-57/S-63 Scheme and for a new S-100 and e-Navigation environment.

Justification and Impacts

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.

Action Required of TSMAD and/or DIPWG

The S-100WG are invited to:

a) note the issues presented in this paper,

b) note that, the provision for data security, encryption and cyber security should be included in S-100 for use in S-10X based products,

c) consider what further action is needed.