HSSC16-05.1J

Paper for Consideration by HSSC16

Comments to HSSC16-05.1G "SENC distribution in an S-100 World"

Submitted by:	France, Canada, Croatia, Estonia, Finland, Germany, Latvia, Norway, Poland, Sweden, Republic of Korea, United States and PRIMAR
Executive Summary:	Allowing SENC distribution creates technical and legal weaknesses: products reaching the ECDIS in this way are no longer the certified and signed products issued by the HO, which opens for cyber security risks and blurs legal responsibilities. The IHO Data Protection Scheme (S-100 Part 15) has been developed on purpose to avoid these pitfalls, and should be used without exception.
Related Documents:	HSSC16-03A Status of List of Actions and Decisions from HSSC-15 IHO WEND-100 Principles Resolution 1/2021
Related Projects:	-

Introduction / Background

1. HSSC15/20 (former HSSC14/25, HSSC13/27) has tasked S100WG "*…to consider the SENC delivery issues raised by France, add this work item in its work plan and report at the next meeting (as part of testing activities and the development of S-164) to address and demonstrate, through a security risk analysis on the application of S-100 Part 15, whether the need for SENC distribution is still justified in the S-100 world."*

2. The IHO WEND-100 Principles Resolution 1/2021 states that "*Member States should ensure the use of the IHO Data Protection Scheme (S-100 Part 15) for distribution to mariners, to secure data integrity, to safeguard national copyright in data, to protect the mariner from falsified products, and to ensure traceability*."

3. The S-100 Part 15 security scheme clearly states that "*the Data Client's software application (OEM System) is responsible for authenticating the digital signatures applied to the product files and decrypting the dataset information*" (section 15-4.3). It is also clear that there must be a chain of trust between the dataset at a Data Client (end user) and the identity of the respective Data Server (producer): *"When Data Clients authenticate the identity of digital signatures created by Data Servers the certificates form a "chain" to the SA[1]'s root level identity."* (section 15-4.5).

4. Reminding of IHO resolution 4/2002, applicable to S-57 ENCs, S-57 SENC delivery has always been optional and at the discretion of the Hydrographic Office: *"As an option Hydrographic Offices may allow the distribution of their HO data (ENC) in a SENC format."*

5. PRIMAR members have decided at their last PRIMAR Advisory Committee (PAC) that PRIMAR will not support SENC distribution of S-100 based data.

Analysis/Discussion

6. No evidence was provided to demonstrate the need for SENC distribution in the S-100 world since HSSC13 (2021). Action HSSC 15/20 is still pending.

[1] SA : Scheme Administrator

7. It should be appreciated that S-100 products and services will originate from a multitude of producers, will require highly varying updating frequencies, and will be consumed in ECDIS that have much improved connectivity (as SECOM is mandated for S-100 ECDIS), see e.g. paper WENDWG14-SHF.E from the most recent WENDWG meeting. Any conversion process will add latency and low latency is key for numerous S-100 layers (S-111 and S-104 in Phase1/route monitoring group).

8. The current (S-57) method of SENC delivery loads the product into the SENC outside of the end user system and merges its information content with that of other products, before delivering the SENC to the end user system. During this process, the product is not kept digitally intact, which would be a precondition to be able to verify its original signature in the end user system, i.e. to verify that the information as provided by the data producer has indeed been delivered entirely intact into the end user system. Therefore, this method would not ensure the integrity of the chain of trust from the dataset (exactly as issued by the HO) at a Data Client (end user system) to its Data Server (producer), as required by the S-100 Part 15 security scheme. Furthermore, it would violate the Part 15 requirement that the authentication of the product signatures and the decryption of the information shall happen in the end user system.

9. The digital signature certifies data integrity, non-repudiation and authentication. For member states and for mariners, digital signature guarantees the authenticity and integrity of the official products that enters an ECDIS. SENC distribution does not meet this essential property, which is a major cyber-security breach that should be absolutely avoided especially in a context where cyber security becomes a very challenging issue.

10. PRIMAR's decision is in accordance with above-mentioned points.

Conclusions

SENC distribution is not only unnecessary, but it does not conform with and generates risks for an otherwise robust standard: the IHO S-100 Data Protection Scheme (S-100 Part 15).

There is no need for Member States to engage in a SENC testing process as recommended by HSSC16-05.1G, whereas cyber security and legal issues are thoroughly dealt with by S-100 Part 15, ensuring product integrity and certification of origin all the way through the distribution chain between data producer and end user.

Action required of HSSC

The HSSC is invited to:

a) Note this paper
b) Encourage IHO member states to engage in the S-100 Part 15 implementation
c) Close action HSSC15/20 (former HSSC14/25, HSSC13/27) as proposed in the S-100WG report
d) Consider not to launch any more action, as there is no evidence of the need for SENC distribution in the S-100 world.