Paper for Consideration by HSSC14

Reflections on the future of SENC delivery

Submitted by:	France (Shom)
Executive Summary:	It is highlighted that allowing ashore decryption and conversion of S-100 products into an ECDIS internal format, and delivering data in this format (referred to as "SENC delivery") creates technical and legal weaknesses that should no longer exist in the S-100 era. Indeed, products reaching the ECDIS in this way are no longer the certified and signed products issued by the HO, which causes cyber security issues and blurs legal responsibilities. The solid technical S-100 specifications for signature and encryption have precisely been developed to avoid these pitfalls, and should be used without exception.
Related Documents:	doc. HSSC13 list of decisions & actions dated 31 August 2021 doc. WENDWG11-04.1A Draft Proposal for a new IHO Resolution on WEND-100 Principles doc. IMO Resolution MSC.232(82)
Related Projects:	

Introduction / Background

1. 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*."

2. For S-57 ENCs, SENC delivery was introduced in §5.1 of the IMO resolution MSC.232(82) on the Adoption of the revised performance standards for ECDIS:
"*The ECDIS may also be capable of accepting a SENC resulting from conversion of ENC to SENC ashore, in accordance with IHO TR 3.11. This method of ENC supply is known as SENC delivery."*

3. HSSC13 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."* (Action HSSC13/27)

Analysis/Discussion

4. Hydrographic Offices must have the guarantee that what enters an ECDIS is what has been issued from their production chain, and mariners expect exactly the same. A S-101 ENC or any other S-100 based product, signed by a HO according to the IHO Data Protection Scheme, does guarantee the integrity and authentication of the official products.

5. Recently, it has been discovered that a qualified distributor made an improper use of French S-57 ENCs data. It seems that this distributor took the opportunity of having access to unencrypted S-57 ENCs to include the data into their own products, in breach of copyright and contract. This hopefully isolated incident raises the issue of the integrity of data once it is unencrypted, outside of a secure system such as an ECDIS.

6. In addition, this incident demonstrates that contracts and legal aspects are not sufficient to ensure data protection and the quality of data provided to end users. Even if the problem has been detected in this case, the situation is not nominal and it is reasonable to point out that once you have a standard (S-100 part 15) specifically created to ensure that this situation does not happen, it is appropriate to use it in all situations. Furthermore, it is never desirable to act *a posteriori* (rather than *a priori*), as it is very difficult to

reconstruct the extent of the piracy. The parallel with SENC delivery is obvious: if a S-101 ENC is transformed ashore into a SENC product, it means that it is unencrypted at one moment, even if the new SENC product is re-encrypted before transmission to a ship. During this phase, "anything can happen" to the data, whether intentionally or by accident. The unencrypted data may also be kept as-is on a production hard drive. Perhaps more importantly, the data is no longer signed by the producing authority due to the change in format. As a result, when it finally reaches the ECDIS, there is no longer any guarantee that the data inside the distributed "SENC package" is the exact same data as the S-101 ENC that was issued by the HO.

7. Of course, there may be safeguards put into place, procedures and certification processes, use of type-approved software, to mitigate the risk of compromising the data. Anyway, this is adding an unnecessary weak spot in an otherwise robust chain (S-100 part 15, SECOM, IEC 61174, and so on). The above incident also shows that legal terms (a copyright restriction or a certification process) are not sufficient to protect data integrity.

8. If the cybersecurity risk may seem manageable during the process of transforming a S-100 based product to be delivered in a SENC format, the legal responsibility attached to the SENC product is the main problem. Once a HO allows the delivery of SENC be made from his own data, it basically agrees to share some responsibility with the SENC manufacturer in case of an accident. Proving the contrary involves many evaluations by experts, to identify whose responsibility is implied. Providing only HO-signed and encrypted data to mariners suppresses all difficulty and should be the way forward, as S-100 part 15 was created for that purpose. The WEND-100 Principles Resolution 1/2021 (see above, point 1.) sums it up very well: SENC delivery doesn't protect data integrity, safeguard copyright, prevent falsified products, nor gives traceability. S-100 part 15 does all this by design.

Conclusions

As stated in IHO resolution 4/2002 as amended, SENC delivery is only an option, that has to be allowed by the producing HO. SENC delivery for S-57 ENCs has been allowed by many HOs for several years now, but progress provided by S-100 products leads to question its relevance. Considering the above examples and explanations, it seems reasonable not to extend SENC delivery in the S-100 era.

Recommendations

Should SENC delivery be thought as useful by some, data integrity and legal risks would have to be carefully analyzed.

In such an eventuality this action should fall under the remit of a more appropriate group than the S-100WG which has no skill for legal issues.

Action required of HSSC

The HSSC is invited to:

a) note this paper
b) identify the right IHO body to handle the risk analysis