HSSC6 -05.2B

Paper for Consideration by HSSC

Extending S-63 Digital Signatures beyond ENC

Submitted by:	United States (NOAA)
Executive Summary:	The United States requests that the IHO S-63 Data Protection Scheme be extended to other navigational products other than ENC.
Related Documents:	S-100
Related Projects:	S-100

Introduction / Background

1. The IHO S-63 Data Protection Scheme describes the recommended standard for the protection of ENC information. It defines the security constructs and operating procedures that must be followed to ensure that the data protection scheme is operated correctly and is currently used solely for the encryption of S-57 ENCs. Under S-100, S-63 is also being adopted to ensure the authenticity of S-100 data products by offering product specification developers the option of digital signatures and/or encryption.

Analysis/Discussion

2. While the United States (NOAA) does not encrypt data through its national distribution system, it has been exploring implementing those portions of S-63 that enable the ECDIS to provide expanded metadata that enables Port State Control to easily determine if the mariners ENC's are up-to-date. During our investigation, we found that in order to implement the "products.txt" portion of S-63, we also needed to implement the digital signature scheme as the implementation between ECDIS varied greatly. E.g. some ECDIS could read in the "products.txt" file, while others required a digital signature. Therefore the United States (NOAA) had to expand its project to incorporate the use of digital signatures and utilize the IHO Scheme Administrator's Certificate.

3. In addition, to including digital signatures as part of its ENC distribution mechanism the United States (NOAA) has also investigated added digital signatures to its PDF of the paper nautical chart that it distributes. However, this requires a certificate to be issued by a scheme administrator. Therefore it is entirely feasible that the S-63 certificate issued by the IHO for ENC should be able to be used by other navigational products issued by authorized hydrographic offices.

4. Additionally, S-100 will be utilizing digital signatures for product authentication and references S-63 as the mechanism.

Conclusions

5. Although S-63 is currently only being used for ENC encryption, the HSSC should consider widening the scope of S-63 to allow for the use of digital signatures for other navigational products. This will then enable the hydrographic community to utilize a consistent mechanism.

Justification and Impacts

6. Allowing for the extension of the S-63 Data Protection Scheme to be used beyond ENCs for other navigational products will create a harmonized security mechanism for the entire maritime community.

7. This will also align with S-100 that will use S-63 as the security algorithm for S-100 based product specifications.

8. In addition, this will not create an undo impact on the IHB as they already have the mechanism in place to issue required security certificates.

Action Required of HSSC

The HSSC is invited to:

a. note the paper.

b. agree to extend S-63 to other products beyond ENC.

c. task DPWG or its subsequent working group to review S-63 to make it non-ENC specific.