ENCWG4-05.23

Paper for Consideration by ENCWG4
S-63 new edition to create a new Sub-Data Server participant

Submitted by:	Thomas Mellor (UK)
Executive Summary:	Proposal to create an S-63 Sub-Data Server, with the ability to sign supplementary files in an ENC exchange set
Related Documents:	S-63 edition 1.2, Paper ENCWG3-5.8.1

Background

During the ENCWG3 meeting Hannu Peiponen, IEC TC80 Chair presented (ENCWG3-5.8.1) *'S-63 needs extension of authentication'*. The paper highlighted a possible cyber vulnerability in ENC exchange sets as there are several files that carry no authentication signatures. The following files in an ENC exchange set have no signatures.

DATA: Axillary txt and tif files – Should be signed by data server

CATALOG.031
README.T XT
PRODUCTS.TXT
MEDIA.TXT
SERIAL.ENC
STATUS.LST

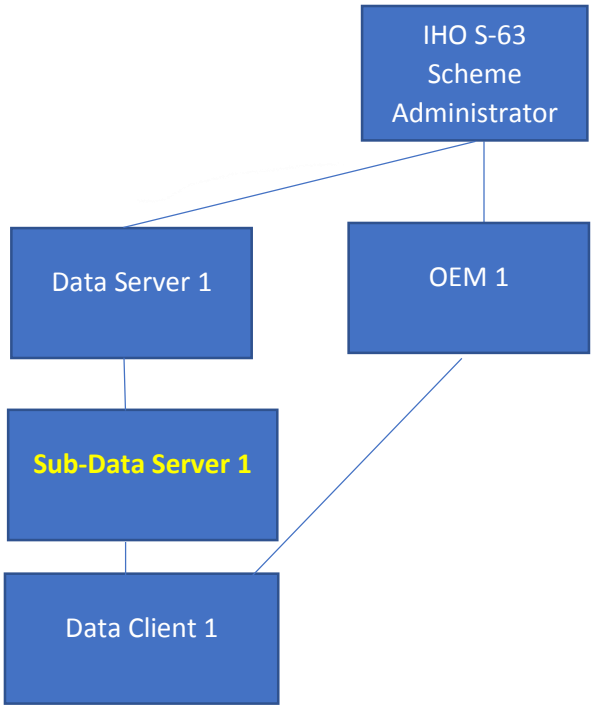
The recommended to address the issue was that S-63 data server should sign these files.

Analysis/Discussion

Unfortunately, this proposal does not support the current ENC distribution model as there are instances where S-63 data servers, pass the Global ENC exchange set to sub-distributors for onward dissemination to the data client. As part of their value-added services sub-distributors will create a weekly bespoke exchange set for the vessel only transferring via satellite communication the navigational data required. This keeps the cost of data transfer down to a minimum and provides the mariner with the best ECDIS user experience as they are only loading data into the system that is required for safe navigation. In this process none of the ENC data is compromised and the authentication signatures on the data files remain untouched. However, the CATALOG.031 is recreated to reflect the exact contents of the bespoke exchange set. This must be done, or it would lead to error messages during the import of the ENC data which would confuse the ECDIS user and create a lot of unnecessary support cases. It is therefore important that sub-distributors have the ability to sign supplementary files in an ENC exchange set.

Recommendations

In order to preserve the current ENC delivery process in use today and to address the cyber security concerns raised it is proposed that S-63 be extended to create a new participant in the scheme, a Sub-Data Server. A Sub-Data Server must be able to create a digital signature to sign the CATALOG.031. They would go through the same registration process with the IHO as a Data Server but would only sign supplementary files not ENC data. They would be restricted to this activity and would not be permitted to create and distribute ENC permits or data. The registration process could also include a recommendation from the current IHO Data Server to the scheme administrator that they appoint the Sub-Data Server. Currently it is estimated that there are approximately 100 companies that may wish to sign up through an existing Data Server to become a S-63 Sub-Data Server.



As stated all Sub-Data Servers appointed by a Data Server must apply to the IHO to be part of the S-63 security scheme. In the same way that a Data Server applies to be part of the scheme the Sub-Data Server must send the IHO a public key and Self Signed Key (SSK). If accepted the IHO would sign the SSK with its private key to produce a Sub-Data Server Certificate.

With any change of this magnitude to an existing IHO standard there will inevitably be an impact on industry. Before any change is made detailed consideration must be given to the impact on ECDIS and the subsequent software upgrades this would necessitate. These changes and the cyber vulnerability that is being addressed must be balanced against the cost to OEMs and ECDIS users.

Action Required of ENCWG

The ENCWG is invited to:

a. Agree the proposal to create an S-63 Sub-Data Server appointed only to sign supplementary files not to create permits or sign ENC data.
b. Carry out an impact assessment to understand the size and scale of the proposed change on ECDIS and the SOLAS industry