Paper for Consideration by HSSC 15

Review of IHO S-100 Security Scheme appointment, operation, and termination process

Submitted by:	UKHO
Executive Summary:	The paper is seeking a review of the procedures for the appointment, operation, and termination process of all participants in the new S-100 security scheme
Related Documents:	S-100 Part 15
Related Projects:	S-63 data security scheme

Introduction / Background

Digitalisation of the shipping industry continues to grow year on year, a trend underpinned by growth in Low Earth Orbit satellite communication networks. Digitalisation is essential for delivering increased navigational safety and operational efficiencies. However, with the rise of cybertechnology comes the increased threat of cyber-attack. Interconnecting or networked systems can lead to vulnerabilities being exposed which increases the cyber-risks for vessels at sea but also shoreside shipping company operations. Cyber-attacks can leave vessels without key navigational safety systems and disrupt shipping operations. The financial cost of recovering from an attack can be catastrophic for shipping companies.

It is well documented that mariners are required by IMO to keep their ECDIS up to date with the latest ENCs for their intended voyage. This transfer of data from shore to the primary navigation system represents a risk to a vessels ECDIS and, if connected via a network, to all concatenated systems.

Over the last 20 years the IHO data protection scheme, S-63, has been used as the primary means of securing ENC information and maintaining the integrity of an ENC service.

The scheme allows ECDIS to provide the mariner with assurance that the ENC data has come from an approved source. It protects the data produced by Hydrographic Offices from piracy through encryption preventing unauthorised use and it provides a mechanism for ENC service providers to license the use of ENC data in ECDIS and other compatible systems.

The IHO Secretariat currently operates the S-63 data security scheme on behalf of Member States by approving applications of data servers and OEMs to be appointed into the scheme.

Analysis/Discussion

As with all security schemes, you are only as strong as your weakest link. At the time of writing this paper, there are just under 400 registered developers subscribed to the IHO S-63 manufacturer list who have all been granted credentials that allow them to develop S-63 compatible systems capable of receiving and displaying encrypted ENCs.

The IHO Secretariat is aware that the contact details on record for these companies is not up to date. Over the last year the ENCWG has attempted to contact all OEM members of the S-63 scheme with woeful results.

With so many OEM participants in the scheme and no way of monitoring them against their signed agreements, the risk of ENCs being misused is extremely high. Infringements of Hydrographic Offices intellectual property is a navigational safety issue and can obviously lead to a loss of revenue.

In contrast there are only thirty-eight IHO data servers tasked with delivering S-63 encrypted ENC services to equipment capable of decrypting the charts.

It has been noted there are many GIS software manufacturers who form part of the S-63 security scheme, and the UKHO are increasingly concerned that software of this type can be used to facilitate ENC users breaching EULAs, as many of these packages allow the ENCs to be saved and exported in other data formats.

Experience of operating an S-63 security scheme has recently highlighted several weaknesses in the chain that need addressing. A number of these are administrative and process-driven rather than technological.

For the administration of the S-100 data protection scheme there is a need to revisit the appointment, running and termination processes for data servers, OEMs and ENC service providers.

Recommendations

It is recommended that the HSSC forms a special project team to assist the IHO Secretariat with developing the S-100 appointment and termination process for data servers, OEMs and ENC service providers. The Project Team should be made up of HOs, OEMs and cybersecurity industry specialists, to ensure any vulnerabilities are addressed in the new S-100 security scheme. This could constitute the reconvening of the Data Protection Scheme Working Group (DPSWG) with additional external support.

The creation of S-128 catalogue files by ENC service providers will necessitate a new appointment process and agreement so these files can be digitally signed.

It is recommended that the aging S-63 OEM and Data Server agreements are reviewed to ensure the contracts are legally binding and provide the IHO with means to terminate if participants are found to have breached their terms. The process for managing the agreements and procedures (necessary to carry out actions if any breaches are found) must be documented.

To support S-100 testbed activities, it is recommended that the IHO only issue a set of generic test credentials to OEMs using S-100 edition 5. Only when new S-100 compatible systems are ready for commercial production would the IHO release the final manufacturer codes on production of a valid type approval certificate or similar. This process would have to be determined for systems not subject to a type approval regime.

The PT/WG should consider if an annual inspection regime for participants within the S-100 security scheme is required, this review would be used to ensure compliance with the agreements. A regular inspection would ensure the integrity of the scheme remains robust with only participants that are manufacturing secure equipment remaining on the scheme. The cost of the inspection would be covered by the scheme participants. The concept of an annual inspections for equipment manufacturers is already a reality being conducted under the EU Marine Equipment Directive to ensure compliance.

Justification and Impacts

To mitigate the risk of cyber-attacks on ships, the IHO must endeavour to ensure the new S-100 security scheme is robust and that all the administrative aspects of the scheme have been assessed and reviewed.

This is a high priority task for the IHO to complete as we need to appoint the relevant actors into the scheme to be able to distribute and use the new S-100 data products on compatible display systems.

There is a clear need to have the new S-100 security scheme in place by the time S-100 product specifications are reaching their operational maturity level. To ensure minimal delays, the administrative aspects of the scheme must be documented and in place by HSSC 16.

To ensure the agreements IHO have in place for S-100 security scheme are legally binding and enforceable, there is a need for specialist legal support. This could be provided by Member States if available or, if this is not forthcoming, then it would be necessary for the IHO to purchase this support.

Action Required of HSSC 15

HSSC 15 is invited to:

a. Form a specialist PT to support the IHO secretariat drafting the S-100 scheme participant appointment, operation process

b. Using legal expertise conduct a review of the existing OEM and Data Server agreements to ensure they are fit for purpose

c. Develop S-100 security scheme termination process for all scheme participants

d. Develop procedures to monitor agreements for possible breaches, including annual inspection regime

e. Develop appointment process for ENC service providers so they can digitally sign S-128 files