Hydrographic Services and Standards Committee

Application of S-100 Data Protection

Document HSSC11-05.1H

Robert Sandvik, PRIMAR and ECC

Principal activities and achievements

- PRIMAR is developing S-100 based services
    - Distribution of S-102 bathymetric data
    - Dual-fuel S-57 and S-101 ENC distribution services
- PRIMAR services will be protected and all files will be digitally signed
- S-100 edition 4.0.0 published December 2018
- New S-100 Part 15 – Data Protection Scheme
    - Defines recommended algorithms and data formats for encryption and digital signatures for S-10x products

S-100 part 15 highlights

- S-100 Part 15 is NOT backward compatible with S-63
  - Change in encryption algorithms and key lengths
  - End-user identification (HW_ID, M_ID, M_KEY) with extended field lengths
  - Better harmonisation with international security constructs
  - Encryption and digital signatures can be used independent of each other
  - Applicable for use by all S-100 based product specifications
  - Each product specification must specify how S-100 part 15 elements are to be used and included in exchange set

Principal activities and achievements

- IHO will be operating as S-100 protection Scheme Administrator
  - Same role in S-63 Data Protection Scheme
  - Create Data Server Certificates and issue Manufacturer information
- PRIMAR S-101 project is developing an IHO S-100 Scheme Administrator application
  - Verify Data Server Certificate Signing Requests (CSR)
  - Create Data Server Certificates
  - Functionality to digitally sign IHO files

Principal activities and achievements

- IHO S-100 Scheme Administrator Application
  - PRIMAR development completed and tested internally
  - Invited external companies for testing
  - Training material for IHO completed
  - IHO to create S-100 root public key (SA Application)
- PRIMAR is developing encrypted S-101 testdata
  - Internal testing in progress
  - Will invite external companies for testing
  - Similar process for S-102 testdata

Problems or outstanding issues

- Identified S-100 part 15 document improvements/clarifications
  - Will create report recommendations to S-100 Data Protection Project Team
- Must make verified testdata freely available (S-101, S-102++)
  - Current plan is to publish PRIMAR testdata on Github until alternative IHO source is available
  - Testdata mandatory for software developers to develop support for S-10x products
- Must amend S-63 OEM and Data Server Agreements to support S-100
  - PRIMAR is reviewing agreements and will be recommending text changes

Action requested of HSSC

- Note the report
- Inform relevant IHO Working Groups of activities and liaise with PRIMAR for any coordination activities