Notes

Development of an IHO Data Protection Scheme

By Robert Sandvik, PRIMAR Stavanger, Norway

Primar and its successor PRIMAR Stavanger have developed and applied security to guarantee a secure and reliable delivery of its ENC services into the market. Time has been spent with equipment manufacturers to advice them on the use of security so they can implement functionality to support the secure ENC services. ECDIS (Electronic Chart Display and Information System) and ECS (Electronic Chart System) manufacturers worldwide have developed support for the security scheme. The wide use and industry acceptance of the PRIMAR Stavanger security standard has basically made it a de-facto industry standard for delivering secure ENC data to the ECDIS/ECS market. Other RENCs (Regional ENC Co-ordinating Centers) and HOs (Hydrographic Offices) are also using the same security scheme to deliver its ENC services or are in the process of evaluating the scheme.

The IHB (International Hydrographic Bureau) has also completed a questionnaire among its member states to review their view on adopting an ENC security scheme (ref. IHO Circular Letter 15/2001). All respondents confirmed it was their intention to have their ENC data supplied in an encrypted format, and 83 per cent supported the concept of having one recommended IHO security scheme. More than half of the respondents supported the PRIMAR Stavanger security scheme becoming the recommended IHO standard.

The IHO CHRIS (Committee on Hydrographic Requirements for Information Systems) decided at its meeting in Athens 2001 to define a work programme for an IHO Data Protection Scheme Advisory Group (DPSAG) to prepare a plan to enable the development of an IHO ENC Data Protection Scheme with supporting documentation modelled on the PRIMAR Stavanger Security Scheme. This article presents the plans proposed to IHO CHRIS for review at its meeting in August 2002 on a recommended course of action for the establishment of an IHO Data Protection Scheme (DPS).

The Data Protection Scheme Advisory Group (DPSAG)

Organisation

PRIMAR Stavanger chairs the DPSAG with representatives from other Hydrographic Offices, system manufacturers and type approval authorities. The DPSAG is looking for more active industry representation from ECDIS/ECS manufacturers end encourages them to be involved in the upcoming work.

Requirements for an ENC Data Protection Scheme

The DPSAG has during its meetings and in independent discussions with Hydrographic Offices and system manufacturers tried to identify high-level require-

ments which must be met for an IHO Data Protection Scheme:

- The Hydrographic Offices (HO) and industry want one common IHO Data Protection Scheme to be used by all data providers for secure ENC distribution
- IHB should be the custodian of the Data Protection Scheme and operate as the Scheme Administrator (SA). The scheme should limit the workload on IHB as scheme administrator and custodian of the documentation. (There will always be the option for IHB to outsource this responsibility if its Member States do not believe this is a core IHB responsibility. The issue will be discussed at the IHO CHRIS meeting in August 2002)
- The security scheme should be based on the Primar Security Scheme (PSS) since it already is a de-facto industry standard and incorporates operational experiences, and recommendations provided by the Canadian Hydrographic Service (CHS). There has been advancements in the provision of international security services since the Primar Security Scheme was developed and CHS has recommended with the support from DPSAG to adopt the use of:
  - Open and standardised file formats for the digital certificates, digital signatures and encrypted files
  - Review the key lengths for encryption keys
  - Review application of digital certificates and trust chains by using services of international Certificate Authorities
- Security should be an envelope applied as a wrapper around the hydrographic information. This will ensure the security scheme can be used for securing also other types of hydrographic information and be independent of file format or versions of S57
- The security scheme must be flexible to support operational modes where hydrographic data is signed only, signed and encrypted, or no security is applied to meet individual security requirements of ENC data providers

Proposed Content of IHO Data Protection Scheme

The DPSAG has recommended that the following information must be developed and made available as part of the IHO Data Protection Scheme:

1. Comprehensive documentation defining all the data entities, their format and operational use with detailed examples enabling interested organisations to develop support for the scheme
2. Comprehensive test data set including erroneous test situations to test the implementations. The test data set must be rich in examples to cover all service aspects
3. Provision of a software kernel to ease implementation and provide as a reference code on the use of all security constructs. The software kernel will provide a core implementation of all security constructs covering digital signing and encryption for data delivery, and verification of digital signature and decryption for data use

Developing the IHO Data Protection Scheme

The DPSAG has carefully reviewed the best way forward for developing the IHO DPS. There is a urgent need for some Hydrographic Offices and RENC operators (e.g. IC-ENC) to formalise the adoption of an IHO Data Protection Scheme, but it will also take a few years to prepare an IHO DPS incorporating all the proposed recommendations and allow sufficient time for system manufacturers to develop support for the new standard and install it on all vessels among their customer base.

DPSAG has recommended preparing the IHO Data Protection Scheme in 2 phases and versions to best meet these operational requirements.

Phase I: Since the current Primar Security Scheme (PSS) is already widely used by ENC data providers and system manufacturers, the DPSAG recommends that the current Primar Security Scheme is approved as an IHO Data Protection Scheme version 1. This will ensure an official and international acceptance of the security scheme with an immediate and easy adaptation and use of the scheme by other hydrographic organisations and system manufacturers

Phase II: The DPSAG has a long-term objective to prepare a second version of the IHO Data Protection Scheme incorporating the operational experiences and proposals made by the Canadian Hydrographic Service. This will give the DPSAG sufficient time to review and incorporate the necessary changes to the security scheme. Sufficient time must in addition be set aside for the industry to incorporate these changes into their systems and upgrade their installations among its customers. This will also be the only amendment to the IHO Data Protection Scheme that can be envisaged since the resistance and cost of more changes will be too high among the ENC data providers and system manufacturers

The proposed plans will be reviewed by IHO CHRIS at its meeting in August 2002 and any recommendations or revisions by IHO Member States will be incorporated in the plans before the work starts.
A proposed high-level plan for the work in the 2 phases is as follows:

Preparation of IHO Data Protection Scheme v.1

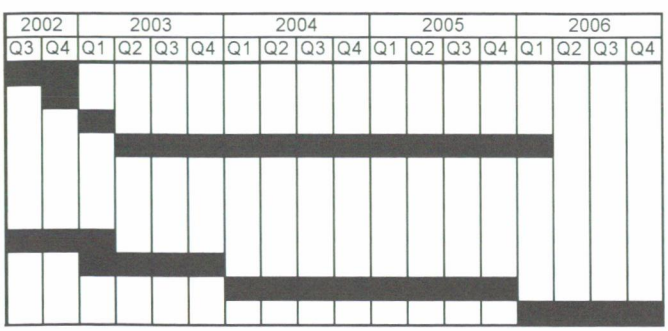
The most important activity in this phase will be to review and prepare the necessary documentation, testdata and software kernel. None of the security constructs in the Primar Security Scheme will be changed, but more informative explanations and examples will be provided to remove some ambiguity issues. A software kernel has been developed by the Canadian Hydrographic Service covering all functions required to encrypt and digitally sign the ENC data, together with the decryption and verification of the digital signature.
When the scheme administrator role is transferred to IHO, a new scheme administrator digital certificate will be issued by IHB. All ENC data providers will be using a digital certificate derived from the scheme administrator certificate. Some equipment manufacturers have not implemented functionality to properly handle multiple digital certificates despite the procedures defined in the current security documentation. PRIMAR Stavanger is working with the UK Hydrographic Office to resolve this issue with the industry before the scheme administrator role is transferred to IHB. The number of non-compliant ECDIS/ECS installations has gone down from 40 per cent in April to 15 per cent in June 2002.
The scheme administrator role will be transferred to IHB when the IHO Data Protection Scheme documentation is available and all security issues with the industry has been resolved and proved operational during the Spring 2003. It is estimated that the workload on IHB will be less than a man-month each year to operate the IHO Data Protection Scheme.

Preparation of IHO Data Protection Scheme v.2

The DPSAG has identified several study items that will be reviewed during the remainder of this year. A new working group meeting is scheduled early 2003 to review the conclusions from these studies and discuss how it can best be incorporated into the next version of the IHO Data Protection Scheme. The DPSAG excepts it will be possible to develop the software kernel in parallel with writing the documentation to review the operational feasibility and as an important quality control element of the standard. Another advantage to such a process is that the test data and software kernel will be prepared during the process and available at the same time as the documentation.

Phase I
IHO Data Protection Scheme v.1
Resolve security issues with industry
Prepare documentation, testdata, software kernel
Transfer scheme administrator role to IHB
IHO DPS v1 in operation by IHB

Phase II
IHO Data Protection Scheme v.2
Review solutions for proposed changes
Prepare documentation, testdata, software kernel
Develop and install systems supporting IHO DPS v.2
IHO DPS v.2 in operation



It is expected that the workload on IHB will be very limited since it is envisaged the new version of the security scheme will be based on widely accepted international security constructs and services.
Approximately 2 years have been set-aside for the ENC data providers and system manufacturers to implement the new version of the security scheme. This should be feasible considering it is building on the Primar Security Scheme and that it will utilise standardised formats and services which various software libraries also support. Both versions of the security scheme will be supported during a limited transition period before support for version 1 is terminated. The proposed transition procedure must be carefully reviewed and agreed with representatives from industry and ENC service providers.

E-mail: robert.sandvik@ecc.as