CHRIS15-7B

15th CHRIS MEETING
IHB, Monaco, 10-13 June 2003

IHO ENC SECURITY SCHEME
(by IHB)

Note: Click on yellow shaded text to obtain more information

With a view to handing over the Primar Security Scheme (PSS) to the International Hydrographic Organization (IHO), a training of two IHB Professional Assistants (Anthony Pharaoh and Michel Huet) by staff from Electronic Chart Centre AS (ECC), Norway, took place at the IHB, Monaco, on 24-25 April 2003.

Developed by Primar Stavanger in cooperation with Hydrographic Offices, the PSS has been run by ECC from 1998-2003. At the end of 2002, IHO Member States approved that the PSS be made Version 1 of the IHO Recommended Security Scheme for ENC (RSS) and that the role as Security Scheme Administrator be transferred to the IHB. This was reported in IHB Circular Letter 66/2002.

Description of the IHO RSS will appear in IHO Publication S-63, of which a draft was prepared and reviewed on the occasion of a meeting of the IHO/CHRIS Data Protection Scheme Advisory Group (DPSAG) that was held, also at the IHB, on 13-14 March 2003. Some parts of S-63 still need completion and it is planned to publish it by end of May 2003. S-63 includes the documentation describing the Standard and two appendices dealing with associated test data sets and software kernel.

The IHB will act as certification authority for Ver.1 of the IHO RSS. In effect, the RSS generates digital signatures by means of a mechanism known as Digital Signature Algorithm (DSA) whereas the Blowfish system is used for ENC encryption. However, most of the recognised Certification Authorities have adopted an algorithm mixing digital signatures and encryption, like RSA. While Ver.2 of the IHO RSS will likely make use of the RSA system, the DPSAG considered it would be wise to keep the current system for the time being, i.e. DSA, as the implementation of RSA on all ECDIS/ECS using the PSS/RSS would require a significant amount of work by manufacturers in a short time.

A key element of the training session was therefore the generation of a scheme administrator certificate. Other aspects were the creation of data server certificates, e.g. for Primar Stavanger and all Value Added Resellers (VAR) of IC-ENC, and the creation of appropriate keys (known as M_ID and M_KEY) for ECDIS manufacturers, that will authenticate ENC signatures and decrypt ENCs.

It is planned that the official handover will take place during the IHO Industry Days in Monaco on 16-17 June 2003. The ENC distribution security norm will then change its name from PSS to the IHO S-63 Standard, which will become the official Hydrographic Standard for secure distribution of ENCs to end users. This standard has already been adopted by several RENCs and distributors.

Seventeen of the 30 OEMs which collaborate with Primar Stavanger already have type approved ECDIS systems compatible with this standard. It is anticipated that the transfer should have no or very little impact on end users.

The handover of the PSS to the IHO should mark a milestone in the development of ENC services, and it is hoped that many HOs, RENCs and ENC producers will begin incorporating S-63 security in their services – creating the first seamless standard which removes some of the uncertainties in developing ENC services.

See also Doc. CHRIS15-6.3A.