

**2<sup>nd</sup> IHO-HSSC Meeting  
Rostock, Germany, 26-29 October 2010**

**Paper for Consideration by HSSC**

**Proposed Amendment to IHO Publication S-63.**

<b>Submitted by:</b>	HNHS, Greece
<b>Executive Summary:</b>	This paper proposes an amendment to the IHO S-63 Data Protection Scheme in order to include Academic Research Users as participants to the S-63 scheme.
<b>Related Documents:</b>	a. IHO S-63 Data Protection Scheme

### **Introduction / Background**

1. When an academic institution purchases ENC and RNC data strictly for academic and research purposes, it should not be required to sign the industry OEM agreement, but a special agreement, granting an unlimited time use license and the option to select or not the purchase of update service.

### **Analysis/Discussion**

2. The Cartography Laboratory of National Technical University of Athens (NTUA) has recently signed a contract with 7Cs for the procurement of a Software Development Kit (SDK) and some ENC and RNC data. In the correspondence with 7Cs it has been clearly and repeatedly stated that the purpose of the procurement of the SDK and the accompanying ENC and RNC data is to use them for academic research, such as the support of lectures, theses and dissertation topics, in the Cartography Laboratory of the NTUA. The Cartography laboratory of the NTUA does not intend to use the SDK for the development and marketing of commercial systems or products and the applications that will be developed with the data are exclusively of academic interest and will not be released for any commercial use.

3. For the abovementioned reasons, NTUA needs ENC and RNC data with a permanent use license without update service. Unfortunately the procedures of S-63, such as the signing of the IHO-OEM agreement, are aimed for companies that have or wish to develop and market systems (IHO-OEM Agreement, Version 1.1 refers) and therefore cannot be applied in this case. On the other hand it should be noted that NTUA does not have the right to sign such an agreement.

### **Conclusions**

4. IHO Publication S-63, which contains the existing OEM licence proforma, needs to be amended so as to include an additional OEM agreement for "academic" developers.

### **Recommendations**

5. HNHS recommends that IHO S-63 be amended as indicated in the attached draft.

### **Action Required of HSSC**

6. The HSSC is invited to:
- a. **Recommend to Member States** that IHO S-63 be amended as indicated in the attached draft as Annex A.
  - b. **Endorse** the proposed IHO ARU Agreement be amended as reflected in the attached draft as Annex B.

## Proposed Amendments to IHO Publication S-63

(The proposed additions have been marked in blue)

- A. Replace the introductory text of section 1.2 by the following (add the academic research user):

### 1.2 Participants in the Scheme

There are several types of users of the scheme, these are as follows:

- The Scheme Administrator (SA), of which there is only one.
- The Data Server (DS), of which there can be many.
- The Data Client (DC), of which there are many.
- The Original Equipment Manufacturer (OEM) of which there are many.
- **The Academic Research User (ARU) of which there are many.**

A more detailed explanation of these terms is given below.

- B. Replace the text of section 1.2.4 by the following (add the academic research user):

### 1.2.4 **Original Equipment Manufacturers (OEM) and Academic Research Users (ARU)**

OEMs subscribing to the IHO S-63 DPS must build a software application according to the specifications set out in this document and self-verify and validate it according to the terms mandated by the SA. The S-63 standard contains test data for the verification and validation of OEM applications. The SA will provide successful OEM applicants with their own unique manufacturer key and identification (M\_KEY and M\_ID).

The manufacturer must provide a secure mechanism within their software systems for uniquely identifying each end user installation. The scheme requires each installation to have a unique hardware identifier (HW\_ID).

The software application will be able to decrypt the cell keys using the HW\_ID stored in either the hard lock or soft lock devices attached to or programmed within the application to subsequently decrypt and uncompress the ENC data. The CRC value contained within the ENC [1] can then be verified to establish the integrity of the underlying S57 data.

**ARUs are university and academia research laboratories that use ENC data strictly for research purposes and not for commercial or operational use. ARUs subscribing to the IHO S-63 DPS are subject to the same requirements and procedures applied to OEMs with the exemption that ARUs are entitled to use unlimited time licenses and the option to select or not the purchase of update service.**

- C. Replace the text of the first paragraph of section 4.1 with the following (add text for ARUs):

### 4.1 Introduction

Data Clients do not buy ENC data but are licensed to use it. Licensing is the method that Data Servers use to give Data Clients selective access to up-to-date ENC cells for a given period of time. **Nevertheless for the promotion of scientific research ARUs are entitled to use unlimited time licenses and the option to select or not the purchase of update service, provided that their applications will be used strictly for research purposes and will not be released for any commercial or operational use.**

OEM/ARU REQUEST FORM



IHO S-63 Data Protection Scheme

**M\_ID and M\_KEY Request Form**

Ed.1-2003

Form to be returned to:

**International Hydrographic Bureau  
4, Quai Antoine 1<sup>er</sup>, B.P 445 - MC 98011 MONACO Cedex  
Principality of Monaco**

Tel: +(377) 93 10 81 00, Telefax: +(377) 93 10 81 40

**Part I: To be completed by OEM/ARU organisation**

**Organisation:** .....

**Address:** .....

**Address:** .....

**Address:** .....

**Postal number/place:** ..... **Country:** .....

**Tel:** ..... **Fax:** ..... **Web:** .....

**Administrative point of contact:**

**Technical point of contact:**

**Name:** ..... **Name:** .....

**Tel:** ..... **Tel:** .....

**E-mail:** ..... **E-mail:** .....

*Please verify the following information is included:*

- All fields in Part 1 of this form are completed
- Signed IHO S-63 Confidentiality Agreement, or  already available with IHB
- Completed successful testing of application with the M\_ID and M\_KEY provided with the S-63 test dataset

**Signed date:** ..... **Name:** .....

**Part II: To be completed by IHB**

- Verify Part 1 is completed
- Signed Confidentiality Agreement available, ref. ....
- Verify OEM/ARU does not have a previously issued M\_ID and M\_KEY
- Assigned M\_ID: ..... M\_KEY: .....
- M\_ID and M\_KEY returned to OEM/ARU and all registered Data Servers

**Signed date:** ..... **Name:** .....

# International Hydrographic Organization

## ARU Agreement

### Version 1.1

THIS AGREEMENT is made this «Day» «Date» by and between the International Hydrographic Bureau (hereinafter referred to as IHB), the Secretariat of the International Hydrographic Organization (hereinafter referred to as IHO), an Intergovernmental Organization headquartered in the Principality of Monaco, and «To» hereinafter referred to as **the University**), **an academic and not profit organization** under the laws of «Country» and having its principal place of business at «Address\_Line1», «Address\_Line2», «Address\_Line3».

### WHEREAS

IHB has coordinated the development of the IHO S-63 Data Protection Scheme and is undertaking the role of Scheme Administrator (SA) on behalf of the IHO.

The **University** has or wishes to develop and use **strictly for academic research and teaching purposes** a system compliant with the IHO S-63 Data Protection Scheme to allow the processing and display of ENC information protected by the Scheme and has requested the SA to provide proprietary information complementary to the IHO S-63 documentation to enable this.

IHB acting as SA has taken note of the request made by the University to participate in the S-63 Data Protection Scheme, in which the University has indicated its willingness to fulfill the testing requirements.

IHB acting as SA is willing, subject to the terms of this Agreement, to provide the **University** with Proprietary Information specific to the **University** to enable systems produced by the **University** to process and display ENC data protected by the S-63 Data Protection Scheme.

The IHO has established the Data Protection Scheme Working Group and an S-63 discussion group to provide a forum for the **University** to put forward experiences with and suggestions for improvement of the IHO S-63 Data Protection Scheme.

## DEFINITIONS

In this Agreement, save where the context otherwise requires, the following terms and expressions shall have the following meanings:

IHB / <a href="#">University</a>	The parties to this Agreement
Cell Key	Key used to produce encrypted ENC, and required to decrypt the encrypted ENC information.
Cell Permit	Encrypted form of Cell key, created specifically for a particular user.
Data Protection Scheme	The set of tools, procedures and definitions to encrypt/decrypt and digitally sign/authenticate signatures to ENC as defined in the IHO S-63 standard using the Proprietary Information.
Data Server	Term used to represent an organisation producing encrypted ENCs or issuing Cell Permits to Users.
ECS	Electronic Chart System, an electronic navigational aid utilising ENCs.
ECDIS	Electronic Chart Display System, type approved navigation system utilising ENCs compliant with IMO ECDIS Performance Standards and IEC 61174.
ENC	Electronic Navigational Chart as defined by the ENC Product Specification in IHO S-57 Data Transfer Format.
EPS	ENC Processing System. An application developed or used by the <a href="#">University</a> to either create protected ENCs compliant with IHO S-63, or to process protected ENCs to display the chart information.
HW_ID	Unique hardware ID known only internally to the EPS application.
IHB	International Hydrographic Bureau. IHB is the operational secretariat of the International Hydrographic Organization.
IHO	International Hydrographic Organization. IHO is an Intergovernmental Organization headquartered in the Principality of Monaco.
M_ID	ECDIS manufacturer's identity provided by the Scheme Administrator.
M_KEY	ECDIS manufacturer's key provided by the Scheme Administrator. Used to create User Permit.
OEM	Original Equipment Manufacturer
Proprietary Information	All information defined in the IHO S-63 Data Protection Scheme required by the OEM to participate in the protection scheme. It includes the Manufacturer ID and Manufacturer Key (M_ID and M_KEY), SA Certificate and Public Key, User Permit, Hardware ID (HW_ID), Cell Permits and Data Server Certificate information, and any other information supplied by or on behalf of IHB, related to the operation of the Data Protection Scheme, and marked as confidential.
SENC	System ENC, the OEM's chosen data format which is created from the decrypted ENC Information, and which the EPS application software uses.

The SENC format applies both to the internal system format used by ECS/ECDIS, or used by the Data Server service delivery system.

SA	IHO S-63 Scheme Administrator. IHB is Scheme Administrator responsible for administrating the Data Protection Scheme, and its operational use on behalf of the IHO.
User	The <a href="#">person(s)</a> who operates the EPS; this excludes personnel employed or hired by the <a href="#">University</a> to service the EPS
User Permit	Encrypted form of Hardware ID as defined in Proprietary Information and in IHO S-63 Data Protection Scheme.

## DUTIES OF THE UNIVERSITY

### General Requirements:

*Ensure, by utilising the IHO S-63 standard, the accompanying guidance notes and the S-63 Test Data Set, that their EPS fulfils the requirements of, and is compliant with the S-63 Data Protection Scheme and the technical requirements of this Agreement.*

*Not state, or infer in any way, that IHO, IHB acting as SA has formally approved the University's implementation of the IHO S-63 Data Protection Scheme; however, the University is able to state that they believe that their EPS is compatible with the IHO S-63 Data Protection Scheme.*

*Notify the SA immediately of any breach or suspected breach of the Security System that it becomes aware of. In such cases, the University shall immediately supply the SA with any necessary detail of the nature of the breach, when it happened, and what ENC information or Proprietary Information is involved in the breach and provide assistance to the SA to identify the cause of any breach.*

*Return to the SA any Proprietary Information that is revoked from the University by the SA and without further notice discontinue any further use of it.*

### Technical requirements:

#### The University must:

*Protect the data contained within the SENC so that it is:*

*Copied and write protected within the EPS (i.e. the SENC becomes useless if copied from one EPS to any other EPS, or if the SENC is amended)*

*and/or*

*Stored in a way that makes it very hard for a user to determine its contents.*

*Not provide any information to Users, whether as part of the EPS, system documentation, or otherwise, concerning where the temporary unprotected ENC file is located within the EPS.*

*Not provide to Users a SENC to ENC conversion programme that exports ENCs originally secured by the S-63 Data Protection Scheme, either in written form or incorporated into the system, or in any way suggest to Users how such a programme could be constructed.*

*Provide a secure form of unique identification for each unit of the EPS manufactured. This "Hardware ID", as defined in IHO S-63, must not be produced using sequential numbers. The "Hardware ID" must be stored within the EPS in a secure way.*

*Keep a register of all Hardware IDs and User Permits (both as defined in IHO S-63) created, and if requested by the SA supply a copy of the register to the SA within 15 working days.*

*Not provide any information to Users, whether as part of the EPS, system documentation, or otherwise, concerning the disclosure or manipulation of the “Hardware ID” information.*

*Produce a User Permit (as defined in IHO S-63) for each applicable EPS manufactured, and ensure this User Permit is freely available to the User.*

The **University** must furthermore ensure that all of their EPS incorporating the IHO S-63 Data Protection Scheme performs the following tasks and meets the following requirements when decrypting ENCs protected by the Scheme:

*Authenticate the SA Digital Certificate prior to loading of the protected ENC information, and prominently display an appropriate message to inform the User if the SA Digital Certificate is invalid.*

*Allow the User to view the SA Digital Certificate / Public Key (as defined in IHO S-63), and to enter a new official Digital Certificate/Public Key issued by the SA.*

*Authenticate the Data Server Certificate contained in the Digital Signature file using the SA Digital Certificate/Public Key information. Authentication must be completed for all ENC information prior to loading and processing of encrypted ENCs. EPS must prominently display an appropriate message to inform the User if the Data Server Certificate is not correctly authenticated.*

*Following authentication of the Data Server Certificate, extract the Data Server Public Key from the certificate and use it to verify the signatures of the ENC data files. Verification must be completed prior to loading and processing the encrypted ENCs. EPS must prominently display an appropriate message to inform the User if an ENC data file signature is found to be invalid.*

*Decrypt the ENC using the appropriate Cell Key. Validate the ENC Checksum after decryption and before conversion into SENC format. EPS must prominently display an appropriate message to inform the User if the ENC checksum is not correct.*

*Only hold decrypted ENC information temporarily before conversion to SENC. ENC Information must only be stored in its encrypted state, or as a SENC. It must not be stored in a decrypted state.*

*Delete the decrypted ENC information immediately upon successful conversion to SENC. If the SENC conversion fails, the system must delete the decrypted ENC information immediately and further processing must be on the encrypted ENC. EPS must prominently display an appropriate message to inform the User about the problem.*

*Do not provide within the EPS a facility to copy the temporary unprotected ENC files that exist after decryption and before conversion to SENC.*

*Store Cell Permits as defined in the Proprietary Information in the same format they were received.*

*Conduct the system date and subscription status checks detailed in the S-63 Documentation, and provide prominent warnings also detailed in the S-63 Documentation when appropriate.*

*EPS must provide support of all error messages or equivalent detailed in the S-63 Documentation.*

## **DUTIES OF THE SA**

- 3.1 IHB acting as SA will maintain the S-63 Data Protection Scheme using the procedures set out in the S-63 standard.
- 3.2 IHB acting as SA will inform the [University](#) of any changes in the Proprietary Information and / or to the S-63 standard.
- 3.3 IHB acting as SA will treat as confidential any proprietary information that is marked as such which is disclosed to the SA by the [University](#) in accordance with this Agreement.

## **WARRANTY**

- 4.1 IHO/IHB warrants that it has taken all reasonable care in constructing and documenting the IHO S-63 Data Protection Scheme, but does not warrant that it is fit for any purpose, whether made known to it or otherwise.
- 4.2 IHO/IHB offers no warranty on the accuracy, completeness, and reliability of how the [University](#) has implemented or Users are operating the Data Protection Scheme in their EPS.

## **LIABILITY**

- 5.1 IHO/IHB and its licensors accept no liability for any loss or damages for any IHO S-63 Data Protection Scheme implementation work undertaken by the [University](#) or its sub-contractors, or for any operational use by Users of the EPS incorporating the Data Protection Scheme.
- 5.2 The [University](#) acknowledges that no promise, presentation or warranty has been made or given by IHO/IHB, its licensors or by any person or company on their behalf regarding the profitability of, or any other consequences or benefits to be obtained from, the disclosure, delivery or use of the Proprietary Information disclosed in accordance with this Agreement. The [University](#) has relied on their own skills and judgement to use the Proprietary Information as a basis for their own development of an EPS compliant with the Data Protection Scheme.
- 5.3 The provisions set out in Clause 5.2 remain valid even if the SA has undertaken tests of the [University](#)'s EPS to verify the [University](#)'s implementation of the technical requirements of the S-63 Data Protection Scheme and this Agreement.
- 5.4 No condition or warranty is given that the IHO S-63 Data Protection Scheme or any part of it will be entirely error free, but IHB hereby undertakes that it will take all reasonable steps to correct as soon as reasonably possible errors which are brought to its attention. IHO/IHB will maintain the Data Protection Scheme using the procedures defined in the IHO S-63 standard.

5.5 Therefore, neither IHO/IHB nor its licensors or any other related company or person will in any circumstances be liable for any damages whatsoever, including, but not limited to, without limitation - damages for loss of business, business interruption or other direct, indirect or consequential loss, arising out of the use or inability to use the Proprietary Information. This exclusion of liability is without prejudice to laws, which cannot legally be excluded or restricted.

## INTELLECTUAL PROPERTY RIGHTS

6.1 IHO hereby represents and warrants that it is the sole owner of all, or has properly licensed necessary, rights, title and interest to the Proprietary Information or constructs in the IHO S-63 Data Protection Scheme, including copyrights, trademarks and other proprietary rights.

6.2 Except for the rights to use the Data Protection Scheme in accordance with this Agreement, the **University** shall have no rights in respect of the Intellectual Property relating to the IHO S-63 Data Protection Scheme and the Proprietary Information. ~~The University hereby acknowledges that it shall not acquire any rights in respect thereof and that all such rights shall belong to IHO or its licensors.~~ Nevertheless for the promotion of scientific research, as well as for teaching purposes the University is entitled to use unlimited time license and the option to select or not the purchase of update service, provided that their applications will be used strictly for teaching and research purposes and will not be released for any commercial or operational use.

6.3 The **University** shall not at any time claim or seek to claim or otherwise hold itself out as owning or holding any proprietary rights, including Intellectual Property Rights relating to the IHO S-63 Data Protection Scheme, Proprietary Information and associated documentation provided by IHB, ~~except the right mentioned in paragraph 6.2 to use the data included in the applications that have been developed strictly for teaching and research purposes, for unlimited time period regardless of the purchase or not of updating service, provided that the data will not be released for any commercial or operational use..~~

6.4 The IHB acting as the SA hereby confirms that there will be no charge to the **University** (e.g. royalties or fees) for the use of the IHO S-63 Data Protection Scheme.

## CONFIDENTIALITY

7.1 The **University** undertakes to securely store the M\_KEY information provided by the SA in accordance with this Agreement and to make all possible efforts to protect this information against disclosure to a third party. Disclosure to a third party may only be made with prior written consent from the SA.

7.2 If the consent to disclose information mentioned in 7.1 above is granted, then disclosure shall only be made when such third parties have accepted in written form the same obligations of confidence to those contained in this Agreement and this is approved by IHB prior to the disclosure.

7.3 The **University** undertakes to ensure the dissemination of M\_KEY information within its own organisation and/or according to the above mentioned consent of IHB to third parties is on a strict “need to know” basis.

## TERMINATION

8.1 The IHB acting as SA has the right, without giving the **University** any right to claim for indemnification, damages etc. to terminate this Agreement with immediate effect and withdraw the **University**'s permission to use the Proprietary Information and participate in the S-63 Data Protection giving the **University** a minimum of one calendar months notice if :

8.1.1 The **University** has compromised the S-63 Data Protection Scheme by disclosing Proprietary Information marked as confidential.

8.1.2 The SA has detected significant errors or inadequacies in the implementation of the S-63 Data Protection Scheme within the **University**'s EPS related to the technical requirements set out in this Agreement or to the security of the Proprietary Information provided under the terms and conditions of this Agreement and if the infringements are not rectified within 60 working days for new EPS units and within one year for existing EPS units of the notification of the infringement or as otherwise so agreed with the SA.

8.2 The **University** may terminate this Agreement at any time giving the SA a minimum of one calendar months notice.

8.3 Upon termination, except for any pre-existing rights, the rights to use the Proprietary Information, and all related information, will be withdrawn.

~~8.4 Upon termination of this Agreement the University undertakes to return to the SA all documents and copies of the Proprietary Information, and all other information in connection hereto which is disclosed in accordance with the terms and conditions of this Agreement. The University also undertakes to permanently destroy all electronic records from media, discs or other devices retained after the disclosure.~~

## LAW AND JURISDICTION

9.1 The following is agreed:

9.1.1 The **University** agrees that any legal proceedings that it institutes against the IHB acting as the SA by the **University** shall be brought in the courts of Monaco and that in this event this Agreement shall be governed by and interpreted in accordance with laws of the Principality of Monaco.

9.1.2 The IHB acting as the SA agrees that any legal proceedings that it institutes against the **University** shall be brought in the courts of the **University**'s country of domicile and that in this event this Agreement shall be governed by and interpreted in accordance with laws of the **University**'s country of domicile.

9.2 This Agreement supersedes any previous agreements between the University and Primar or the IHO/IHB in regard to a security scheme for ENC's and takes effect when signed by both parties, and is done in two equal counterparts, retained by each of the parties.

Signed by:

Authorised Signatory for and behalf of

Date

Signed by:

Authorised Signatory for and behalf of the International Hydrographic Bureau

Date