14th IHO CHRIS Meeting
15-17August 2002, Shanghai, China

Report on Data Protection Scheme Advisory Group Activities

Robert Sandvik <Robert.Sandvik@primar.org>

1 Introduction

The IHO Data Protection Scheme Advisory Group (DPSAG) was established at CHRIS 13 to prepare a plan to enable the development of an IHO ENC Data Protection Scheme with supporting documentation modelled on the Primar Security Scheme (PSS) as outlined in the work programme defined in Annex G to Minutes of CHRIS/13, sent with CHRIS Letter 2/2002.

The Advisory Group (AG) has met twice during this period to review and prepare a plan; an AG meeting in May and during a specific security session at the IHO Industry Days in June. The Electronic Chart Centre (ECC) has chaired the work during this period.

2 Background for an IHO Data Protection Scheme

The advisory group has discussed what the ideal objectives or framework should be for an IHO data protection scheme and has come to the following conclusions:

- The Hydrographic Offices (HO) and industry want one common IHO Data Protection Scheme to be used by all data providers for 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. IHB can alternatively outsource this work under their control.
- The security scheme should be based on the Primar Security Scheme (PSS) taking into account the operational experiences, and consider the recommendations provided in *The Canadian Experience Implementing the Primar Security* System (ref. IHO CHRIS13/8F)
- Security is 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 scheme must be flexible enough to support operational modes where hydrographic data is signed only, signed and encrypted, or no security is applied to meet individual security requirements of data providers.

The DPSAG has carefully considered the best process forward to establish an IHO Data Protection Scheme and is proposing a development in 2 phases:

1. Since the current Primar Security Scheme (PSS) is basically a de-facto industry standard for delivering secure ENC data in the ECS/ECDIS market, the advisory group recommends that the current Primar Security Scheme is approved as an IHO Data Protection Scheme version 1. Both the Primar Stavanger RENC operated by the Norwegian Hydrographic Service and IC-ENC RENC operated by UKHO will be using PSS to secure its products and services. The majority of

OEM manufacturers can already support the current PSS. 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 manufacturers. (Ref chapter 3.1 for further information about the plan)

2. The advisory group has also reviewed the operational experience and independent review by the Canadian Hydrographic Service (CHS) of the PSS (ref. IHO CHRIS13/8F) and propose as a long-term objective to prepare a second version of the security scheme. This version will utilise international developments on security standards and services, and at the same time ease the transition for manufacturers since it will be based on the building blocks of PSS. This process will require a close interaction with industry to get feedback and ensure a smooth transition into the market.

   The advisory group will in particular review the use of:
   (i.) Open and standardised file formats for the digital certificates, digital signatures and encrypted files
   (ii.) Review key lengths and consistent application of checksums (if required depending on selected file formats)
   (iii.) Review application of digital certificates and trust chains by using services of international Certificate Auhorities
   (Ref chapter 4.1 for further information about the plan)

2.1 Content of IHO Data Protection Scheme Standard

The advisory group has agreed that the following information must be made available when developing an IHO Data Protection Scheme:

1. Comprehensive documentation
2. Comprehensive test data set including erroneous test situations
3. Software kernel to ease implementation and provide reference code

All advisory group members have confirmed their interest in participating in the development of a security scheme. The Data Protection Scheme must be issued by IHO.

3 Transition of Primar Security Scheme to an IHO Data Protection Scheme v.1

The advisory group has agreed that there is no need to change the current PSS documentation except changing the layout into an IHO format. The ECC will however review the current documentation based on comments from CHS to remove any ambiguity and provide a better explanation of applicable security constructs. The current documentation defines the roles and responsibilities by all participants for an operational security scheme.

The kernel developed by CHS, ref. IHO CHRIS/13/8F will be used to support the IHO Data Protection Scheme. It will be reviewed and tested by ECC. A more comprehensive test dataset will be developed by ECC.

3.1 Outline plan for establishing IHO Data Protection Scheme v.1

The plan (attached) and activities required to hand over the Scheme Administrator role to IHB will be initiated if and when IHO CHRIS decides to approve the plan.

If IHO CHRIS adopts the plan, CHS and ECC will amend the documentation, software kernel and provide a more comprehensive test data set. It will be reviewed before submission to IHB. (Ref. Task IDs 2-8).

In parallel, UKHO and the current Scheme Administrator are already in a dialogue with some OEMs to ensure they properly implement all the features defined in the security scheme, ref. section 3.2. UKHO has reported that approximately 40% of the current security compatible OEM/ECDIS installations were not fully compliant in April, which has been reduced to 15% in June. It is expected that all installations will be compliant by the end of this year. (Ref. Task IDs 10-13).

The actual roll over of the Scheme Administrator role starts with the creation of a new SA private/public key pair to be used by IHB. It will be used to issue new certificates for the HO and RENC participants of the scheme. This will especially apply to the Primar-Stavanger and IC-ENC RENCs. Approximately 2-3 months after a successful operation of the security scheme has been verified (prerequisite to reduce the workload on IHB), ECC will hand over a procedural handbook and provide training of the applicable IHB staff in all required procedures. The formal roll-over of the SA responsibility will be at the end of the training. ECC will continue to provide technical support to IHB when required. (Ref. Task IDs 15-20).

The plan ensures that the workload on IHB will be minimised (see section 3.3) and that they will take over the SA role of a scheme that is proven operational.

3.2 Erroneous implementation of PSS by some OEMs

The handover of the scheme administrator role from ECC to IHB will take place after a possible contentious issue has been resolved with the industry. The problem is related to:

- Currently ECC as SA and Primar Stavanger are using the same private/public key pair to sign their data. (This was also the situation when Primar was in operation). Scheme administrator and Primar Stavanger should use separate private/public key pairs to deliver their services. Will be achieved when the scheme administrator role is handed over to IHB who will be using their own private/public key pair.
- The OEMs must be able to manage certificates issued by the SA. Some OEMs have not implemented this functionality as described in the current PSS documentation. The consequence is that approximately 15% of security compliant ECS/ECDIS installations can today only verify signatures issued by the SA (was 40% in April as reported by UKHO).

The problem is being prioritised by the SA, Primar-Stavanger and the UKHO RENC in cooperation with the affected OEMs and we hope it will be solved shortly. A continuous dialogue and support is available to OEMs to ease the transition.

3.3 Transition and workload for IHB as Scheme Administrator

ECC will provide sufficient training, required software tools and operational procedures to IHB to take over and manage the scheme administrator role. A worst case estimation will require IHB to provide approximately 1 man-month of resources a year to operate the scheme administrator role. A more likely resource requirement will be 2 man-weeks a year.

An alternative to IHB operating as the scheme administrator will be to outsource these activities to an independent company to deliver these services under contract.

4 Development of IHO Data Protection Scheme v.2

The development of IHO Data Protection Scheme v.2 will be to amend version 1 with results from international developments on security standards and services and base it on the current security building blocks.

It is proposed to organise the development of version 2 as a sub-working group in CHRIS Technology Assessment Working Group (TAWG). Draft Terms of Reference is attached for review by IHO CHRIS.

Several work items have been identified which will require further studies. The findings from these studies will be used to develop the next version of the standard. It will be very important to have a close dialogue with the industry and classification societies to ensure market acceptance and ease the transition of the standard into the market. More OEMs, classification societies, distributors/VARs are requested to join the DPSAG to participate in this work. The recommendations from these studies will be used to define the amendments to the standard to prepare the Data Protection Scheme version 2. It is envisaged that this is the only attempt IHO has in developing a Data Protection Scheme. The preparation of new documentation will be done in parallel with developing a software kernel to verify all technical issues and prepare appropriate testdata.

External funding for developing a software kernel should be investigated to ensure a timely developments since none of the current advisory group members have committed resources to this task since the scope and workload is currently undefined..

4.1 Outline plan for developing IHO Data Protection Scheme v.2

The working group agreed on the following plan (attached) to develop IHO Data Protection Scheme v.2.

The working group will prepare documents about its plans for developing version 2 of the security scheme for review by IHO CHRIS (ref. Task IDs 2-6).

Upon approval, the list of study items will be reviewed and working group members will be asked to prepare recommendations on how it can be implemented in the next version of the security scheme. A meeting between the working group members is planned early next year to review the findings and agree the skeleton of the new version of the security scheme (ref. Task IDs 10-11).

The working group members will prepare the documentation, software kernel, testdata and a procedure handbook for IHB. This development will need a close e-mail cooperation between the working group members. It is expected that the IHB workload and procedure handbook will be very limited since it is envisaged the new version of the security scheme will be based on international standards and PKI-services (ref. Task IDs 12-16).

The plan indicates that the industry will have approximately 21 months to implement the new version of the security scheme. This should be sufficient considering that it will build on the current Primar Security Scheme and that it will utilise standardised formats and services which various software libraries also support. During a 3-month transition period, both versions of the security scheme will be available before support for version 1 is terminated. The proposed transition procedure must be reviewed and agreed with representatives from industry (ref. Task IDs 19-22).

During this development process, the working group will maintain a close relationship and provide input to applicable IEC/IMO working groups as requested (ref., Task ID 9).

5 Action Required of CHRIS

The DPSAG members request IHO CHRIS to carefully review the attached Draft Terms of Reference and approve the attached plans to develop an IHO Data Protection Scheme in 2 phases to immediately enable the use of one common security scheme by other hydrographic offices, RENCs and distributors.

IHO CHRIS is also requested to carefully review the transfer of the Scheme Administrator role to IHB. The recommendation is to enable IHB to take on this responsibility, or alternatively let IHB outsource this work. It is expected that possible workload for IHB will be less for the proposed version 2 of the IHO Data Protection Scheme compared with version 1.

Draft Terms of Reference for
Data Protection Scheme Advisory Group (DPSAG)

1. Objective

To develop and maintain an IHO ENC data protection scheme.

2. Authority

This Advisory Group (AG) is a subsidiary of the IHO CHRIS Technology Assessment Working Group (TAWG). Its membership and decisions are subject to IHO CHRIS approval.

3. Procedures

a) The AG should:

(i) Enable immediate preparation of an IHO ENC Data Protection Scheme v.1 with documentation, software kernel and test data modelled on the Primar Security Scheme.

(ii) Review international developments in security services to amend and prepare IHO ENC Data Protection Scheme v.2 with industry representatives and other ECDIS standardisation bodies, and allow for a structured transition of the standard into the market.

b) Develop procedures and information to enable IHO to assume responsibility of the documentation and supporting information and operate as the Security Scheme Administrator. Identify how technical support will be made available to IHO.

c) The AG will liaise and harmonise with other international ECDIS-related bodies as appropriate;

d) The AG should work by correspondence, and use group meetings, workshops or symposia only when required.

e) The AG should identify a work programme for each year, including expected time frame.

4. Composition and Chairmanship

f) The AG shall comprise representatives of IHO Member States (M/S) and Expert Contributors.

g) Decisions should generally be made by consensus. If votes are required on issues or to endorse proposals presented to the AG, only M/S may cast a vote. Votes shall be on the basis of one vote per M/S represented.

h) Expert Contributor membership is open to entities and organisations that can provide a relevant and constructive contribution to the work of the AG.

i) The AG shall be chaired by a representative of a M/S. The Chairman and the Vice-Chairman shall be chosen by the M/S represented in the AG, for a period of tree years.

j) Expert Contributors shall seek approval of membership from the Chairman.

k) Expert Contributor membership may be withdrawn in the event that a majority of the M/S represented in the AG agree that an Expert Contributor's continued participation is irrelevant or unconstructive to the work of the AG.

l) All members shall inform the Chairman in advance of their intention to attend meetings of the AG.

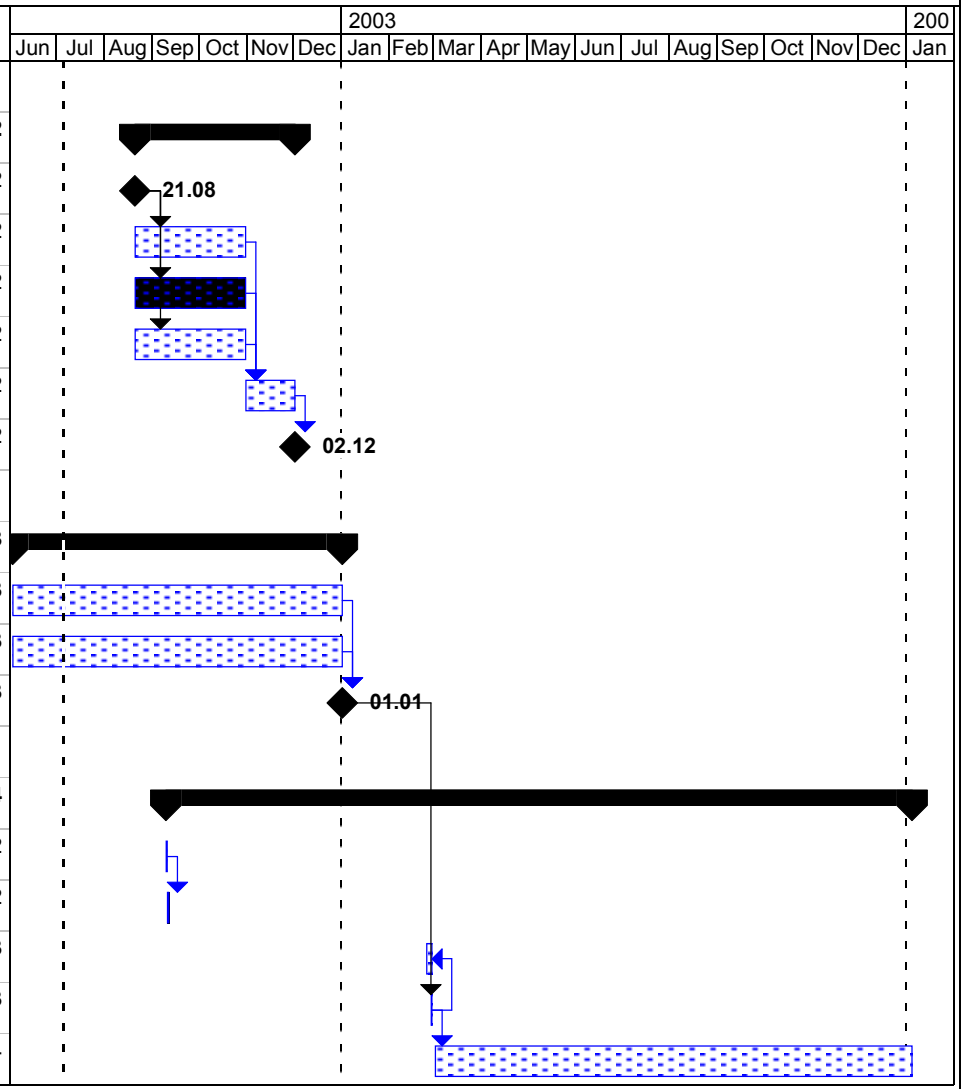
m) In the event that a large number of Expert Contributor members seek to attend a meeting, the Chairman may restrict attendance by inviting Expert Contributors to act through one or more collective representatives.

Data Protection Scheme Advisory Group Membership

Name	***Company***	***Phone***	***Fax***	***E-mail***
Mr Robert Sandvik	Norwegian Hydrographic Service	+47 51 93 95 03	+47 51 93 95 01	robert.sandvik@primar.org
Mr Peter Scott	ECC AS	+47 51 93 95 07	+47 51 93 95 01	peter.scott@ecc.as
Mr Mike Casey	Canadian Hydrographic Service	+1 (613) 995-4666	+1(613) 996-9053	caseym@dfo-mpo.gc.ca
Mr Greg Levonian	Canadian Hydrographic Service	+1 (613) 996-2018	+1(613) 996-9053	levoniang@dfo-mpo.gc.ca
Mr Chris Howlett	UK Hydrographic Office	+44 1823 337900 Ext 3273	+44 1823 284077	chris.howlett@ukho.gov.uk
Mr Raj Alla	IIC Technologies Private Limited	+91-40-335 4806	+91-40-335 6349	rajalla@iictechnologies.com
Mr. Masato Kumada	Japan Radio Company Limited	+81-422-45-9881	+81-422-45-9922	j06573_kumada@m1.jrc.co.jp
Mr Martin Taylor	Kelvin Hughes	+44 208 500 1020	+44 208 559 8524	martin.s.taylor@kelvinhughes.co.uk
Mr Tony Pharaoh	International Hydrographic Bureau	+377 93 10 81 08	+377 93 10 81 40	pad@ihb.mc
Mr Bruno Tréguier	EPSHOM	+33 2 98 22 17 49	+33 2 98 22 03 66	bruno.treguier@shom.fr
Mr Mathias Jonas	Bundesamt für Seeschiffahrt und Hydrographie	+49 40 3190 7330	+49 40 3190 5000	mathias.jonas@bsh.de

Develop IHO Data Protection Scheme v.1

ID	Task Name	Duration	Start	Finish
1				
2	**Prepare IHO Data Protection Scheme v.1**	**78 d**	**21.08.02**	**02.12.02**
3	Review decision at 14th IHO CHRIS meeting	0 d	21.08.02	21.08.02
4	Amend documentation	55 d	21.08.02	31.10.02
5	Amend software kernel	55 d	21.08.02	31.10.02
6	Amend testdata	55 d	21.08.02	31.10.02
7	Review and quality control documentation	23 d	31.10.02	02.12.02
8	Submit security scheme to IHB	0 d	02.12.02	02.12.02
9				
10	**Security implementation by OEM**	**163 d**	**03.06.02**	**01.01.03**
11	Dialogue with OEM industry	163 d	03.06.02	01.01.03
12	Support to OEMs	163 d	03.06.02	01.01.03
13	Proper implementation by all OEMs	0 d	01.01.03	01.01.03
14				
15	**Scheme Administrator role to IHB**	**366,94 d**	**10.09.02**	**05.01.04**
16	Creation of IHB private/public key	1 d	10.09.02	10.09.02
17	Issue security scheme certificates to all RENCs	1 d	10.09.02	11.09.02
18	Training of IHB staff	4 d	25.02.03	28.02.03
19	Actual roll-over of SA role to IHB	1 d	28.02.03	28.02.03
20	Support provided to IHB	234,67 d	03.03.03	05.01.04

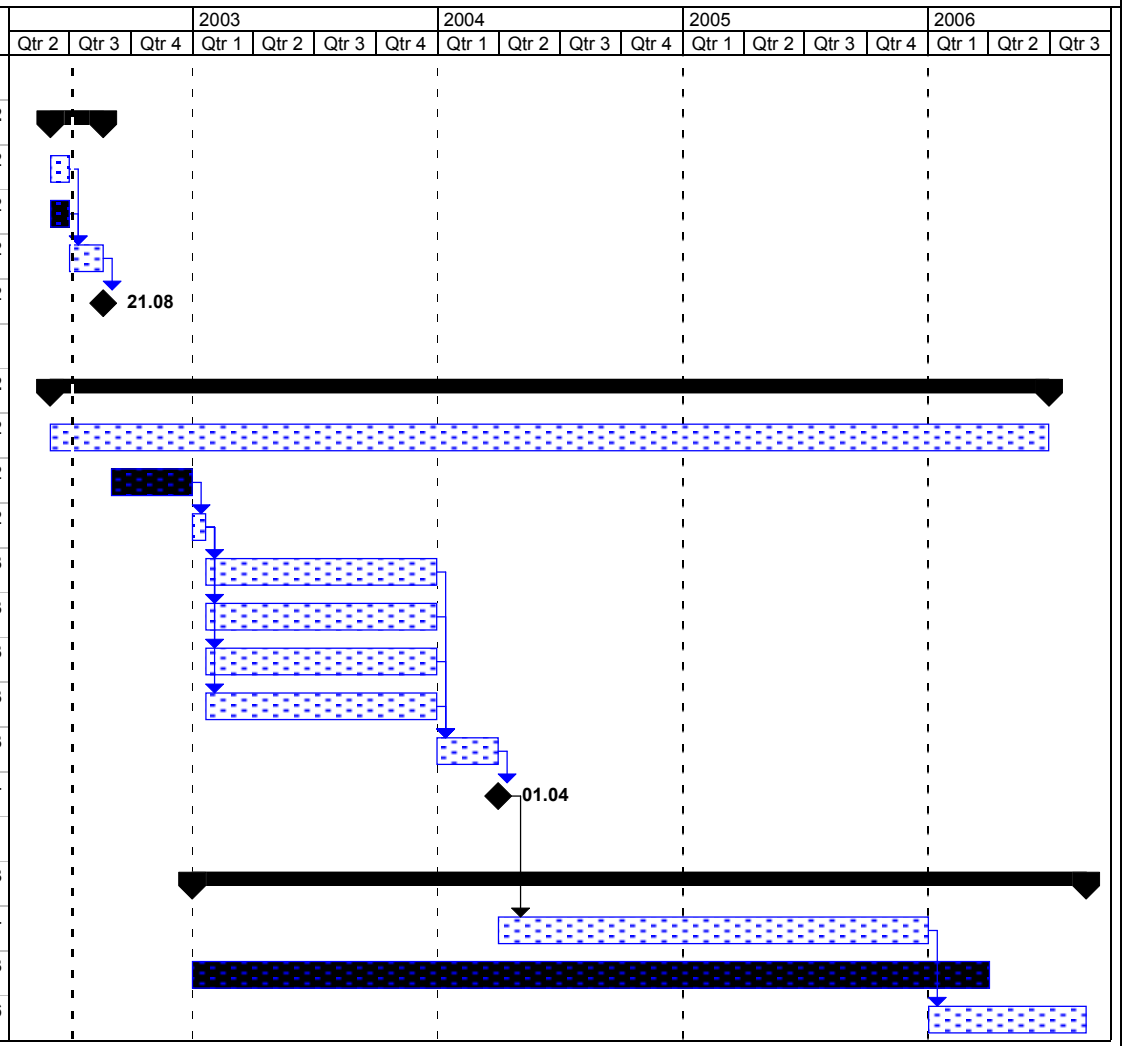


Project: IHO Security Scheme v.1 and
Date: 05.07.02

Task
Split
Progress
Milestone
Summary
Rolled Up Task
Rolled Up Split
Rolled Up Milestone
Rolled Up Progress
External Tasks
Project Summary

Develop IHO Data Protection Scheme v.2

ID	Task Name	Duration	Start
1			
2	**14th IHO CHRIS Meeting**	**61 d**	**03.06.02**
3	Prepare draft Terms of Reference for DPSAG	22 d	03.06.02
4	Prepare development plan for v.2	22 d	03.06.02
5	Review by CHRIS members	39 d	01.07.02
6	CHRIS decision to develop v.2	0 d	21.08.02
7			
8	**Develop IHO Data Protection Scheme v.2**	**1136 d**	**03.06.02**
9	Liaison with IEC/IMO	1136 d	03.06.02
10	Work item studies	92 d	02.09.02
11	Design security scheme skeleton	15 d	31.12.02
12	Prepare documentation	263 d	20.01.03
13	Develop software kernel	263 d	20.01.03
14	Prepare test data	263 d	20.01.03
15	Prepare IHB procedure handbook	263 d	20.01.03
16	Review and quality control	70 d	31.12.03
17	Submit IHO Data Protection Scheme v.2 to IHB	0 d	01.04.04
18			
19	**Set IHO Data Protection Scheme in Operation**	**1015,8 d**	**01.01.03**
20	Implement IHO DPS v.2 in HO/RENC/OEM	488 d	01.04.04
21	IHO DPS v.1 in operation	905 d	01.01.03
22	Set IHO DPS v.2 in operation	180 d	02.01.06



Project: IHO Security Scheme v.2
Date: 05.07.02

Aktivitet
Fremdrift
Milepæl
Sammendrag
Fremhevet aktivitet
Fremhevet milepæl
Fremhevet fremdrift
Deling
Eksterne aktiviteter
Prosjektsammendrag