Report of the IHO DPSWG

Submitted by:	Chairman
Related Documents:	IHO S-63 [all editions], IHO S-100, IEC61174
Related Projects:	NA

Chair:	Jonathan Pritchard, UK
Vice Chair:	Robert Sandvik, Norway
Secretary:	Tony Pharaoh, IHB
Member States:	Australia, France, UK, Japan, Germany
Organisations:	Chartworld/7Cs, Furuno Finland, Transas, IC-ENC, IIC Technologies, JRC, Kelvin Hughes, PRIMAR, SAM Electronics

See Annex A for full details of membership

Meetings Held During Reporting Period

None – Correspondence has been by email and through an online Google collaboration group this year. DPSWG is attempting to draft a new version of the standard (reported below) and the main task in the workplan is the creation of a new edition. A drafting group was planned for 2015 but has not, as yet, taken place due to resource constraints. A revised set of milestones is currently under development for creation of the new edition of the standard.

Planned Meeting

No meetings are currently planned. It is intended to hold a meeting in the early part of 2016. In order to make best use of key stakeholder's time it is hoped that a meeting in conjunction with the S-100 WG and the ENC WG in 2016 is possible. At the moment, discussions with the chair of the S-100WG are under way to progress this. As the group is mainly in "drafting" mode a meeting in March 2016 would be the most appropriate time to consider progress as well as discussing any issues within the wider IHO community.

Work Program Items

Updates to IHO S-63

As reported at the last HSSC, Edition 1.2.0 of S-63 was arrived at by the creation of Annex C of the standard. This edition of the standard is now live on the IHO web page and acts as a normative standard supporting the latest edition of IEC61174.

New Edition of IHO S-63

As reported at the last HSSC, a new edition of S-63 is currently under preparation. In accordance with the previous DPSWG meetings the form of the new edition of the standard is structured as follows:

- **Section A**: Dealing with data encryption, permit generation and information to support data distribution through services.
- **Section B** – Data Authentication, digital signatures and their creation and verification (intended for S-101 but applicable to other S-10x data products as required).
- **Section C** – Dealing with the management and administration of the data protection scheme.

Additionally it is proposed that S-100 and S-101 contain content currently within S-63. Noting the discussion at HSSC6, DPSWG believes this is the optimum way of ensuring maximum reuse for certain elements of S-63 within other S-100 product specifications, whilst at the same time minimising the amount of content required in S-63 itself.

Current drafting efforts have resulted in a structural draft and various group participants are filling in content under the sections defined above. It is estimated this activity will continue until the end of December 2015 followed by a period of review and edit before consideration as a fully-fledged draft in March 2016. A revised version of the draft is periodically posted to the Google collaboration group for update by group members. Although not ideal, progress this year is reflective of the resources available to the group currently and a revised timescale for production of a draft provides the ability to work with fellow stakeholders in the S-100 WG next year.

Support to the Data Protection Scheme Participants and other working groups

The number of OEMs in the data protection scheme currently stands at 275, an increase of 39 from August 2014. This represents a steady growth throughout the year and, as in previous years, mostly represents companies involved in a wide range of activities rather than those purely concerned with ECDIS.

A reasonably steady stream of support questions are received by the IHB and often DPSWG chair provides detailed technical support. There are far fewer of these than in previous years but most notable is an increase of the number of queries about copy protection, cloned dongles and licencing conditions. Many queries relate to permissions for data use and the need for unique hardware id numbers in order to unlock S-63 data. There is a need to highlight

- The scope of S-63
- How the data encryption part of the scheme works
- To Member States the need to think about non-ECDIS use of their data
- The considerable saving in time and energy if common distribution standards covering wider use such as streaming, separate authentication and web presentation are arrived at.

In terms of support to other working groups the biggest single piece of work has been the reviews and updates to S-64 prior to its publication. DPSWG members reviewed the test dataset and associated documentation and worked with TSMAD members and the IHB in order to put the final versions of the document together. S-64 has moved on considerably but we learned some salutary lessons in how difficult the process of review and update for large standards is and how outsourcing some of the proofing, testing and even drafting might save time and energy. A more concrete working environment and processes for large documents and associated test datasets would be a big step forward for all working groups faced with this challenge, particularly as S-100 and its component parts undergo more detailed review and update.

Progress of migration away from IHO S-63 1.0

In August 2015 the IHB prepared a consolidated picture of the status of S-63 1.1's adoption within the ECDIS community as reported by data servers and noted the continuing downward trend of the number of end user

systems still using S-63 1.0. This report is reproduced as Annex B of this document along with four possible options for progressing the situation. It is probably also worth noting that the IHO-EU Network Working Group (IENWG) and CIRM (in response) have prepared reports this year on the wider subject of the updating of ECDIS systems and the implications for users and regulators. It should be recognised that the upgrade to S-63 1.1 is a part of this process and the far wider significance of updating systems at sea. HSSC should consider whether a separate decision is required in respect of the current migration and reporting action on data servers or whether the wider activities under IENWG and CIRM are sufficient to close the remaining gap.

Progress on HSSC Action Items

HSSC6/23	5.2	Extension of S-63 certificates to other navigational products	HSSC6/23	DPSWG to consider the extension of S-63 certificates to other navigational products, and report to HSSC with an assessment of additional resources needed (if any) and potential impact on other tasks and their prioritization.

The question of extension of S-63 to other navigational products has been discussed both within the group, with the IHB, RENC stakeholders and Member States. The following points have been noted and reported here by way of answering this action.

1. IHO S-63 contains much that is ENC specific. File naming conventions, PRODUCTS.TXT, service elements and other aspects tie its use to ENC datasets conformant with IHO S-57. Most of the ENC specific parts of IHO S-63 are within the data encryption and service management parts of the standard.
2. IHO S-63 also splits into 3 distinct parts, the same as those listed previously in this report i.e. Data Protection, Data Authentication and the management of the data protection scheme.
3. The data protection scheme is a trust based enterprise with the IHB performing a valuable role as Scheme Administrator with two main roles: Underwriting the identity of the scheme participants (through the signing of certificates used to produce digital signatures) and the management of confidential codes (used to produce cell permits for the unlocking of ENC data).
4. The key to this issue is to recognise that data encryption and data authentication via digital signatures are completely different and mutually exclusive activities.
5. It is certainly possible to apply S-63 to other types of data to some degree as most of the standard is neutral to the nature of the ENC data. The “spirit” of S-63 could easily be applied to non-ENC data with some minor omissions from the standard.
6. Additionally, the digital signatures can be applied separately from the copy protection for ENC data without modification to the standard. This has been discussed extensively this year. The production of digital signatures requires no confidential information to be shared between the IHB acting as SA and a new scheme participant. Only the need to generate encrypted ENC data should precipitate a formal agreement of confidentiality.
7. The IHB’s ability to verify identity is a key activity in the operation of the scheme. It requires no formal tools and the means by which it is done is poorly documented within the existing S-63 standard

Impacts: The application of S-63 digital signatures (and certificates) to other data products would have the following impacts:

1. A new edition of S-63 would be required which would relax the naming conventions for digital signatures. It would also document the production of signatures and the operation of the identity management of the scheme separately (this is also the approach currently within the new edition of S-63) and would set the scope of the standard wider than ENC data (albeit only for digital signatures).

This would be a fairly major restructuring of the content of S-63 along the same lines as is currently being carried out for S-63 edition 2.0 which is unlikely to be practical with the current resources.

2. Preparation of new agreements which separate the need for confidentiality and the need to verify identity when new participants sign up to the scheme. This would allow new participants the option of signing up produce signed/authenticated data and/or encrypted data. This should not require any additional resource for the scheme administrator but would require a slightly more complex admission procedure to the data protection scheme and the IHBs undertaking of this.
3. Preparation of appropriate test data and documentation including reference implementations against non-ENC data.

Chair DPSWG together with NOAA and the IHB have been through a similar discussion this year and have successfully agreed to produce digital signatures of unencrypted ENC data with their identity assured by the Scheme Administrator but without the need to produce encrypted data and permits. This process and agreement could, in theory, be followed by any Member State wishing to digitally sign and publish signatures of their data and also in order to sign data other than S-57 ENCs.

Problems Encountered

Annex C provides an assessment of the overall status of the work programme.

Resourcing, as always, is a problem encountered within DPSWG. This has been evident this year in the slow progress towards a new draft edition of the S-63 standard for use with IHO S-100. The plan to come up with a new draft outlined in this report should provide something tangible for the next S-100 WG and for submission to HSSC8 as a milestone. Extensive testing and implementation in line with S-101 will need to be considered in 2016 as well. This version should also contain more comprehensive advice on how to implement S-63 across different data products.

Any Other Items of Note

- None

Conclusions and Recommended Actions

Based on the report detailed here the recommended actions for DPSWG are:

a. Continue with the drafting of the new edition of S-63 2.0 in conjunction with the S-100 WG and to find the most optimum locations for each of its component parts
b. Continue to support the data protection scheme participants and IHB in its management of the scheme.

Justification and Impacts

- A new edition of IHO S-63 is required to provide secure and assured communication of S-100 based hydrographic data in the future.
- The overall data protection scheme needs common definitions of e.g. identity, data assurance and description of processes required in order to provide facilities across multiple S-100 data products in the future as well as providing ongoing support for IHO S-57 data.
- There is an ongoing need to provide advice and support to new participants within the data protection scheme.
- The number of participants in the scheme continues to grow.

Action Required of HSSC

The HSSC is invited to:

a. endorse the IHO DPSWG WG report;

b. consider whether a separate decision is required in respect of the ongoing migration to S-63 1.1 and reporting action on data servers or whether the wider activities under IENWG and CIRM are sufficient to close the remaining gap;
c. approve the content, scope and revised timescales of the work plan items provided in Annex D;
d. endorse the continued activity of the WG under its current Terms of Reference.

Annex A

IHO Data Protection Scheme Working Group (DPSWG)
Membership and Contacts (30 June 2014)

Member States	Name	E-mail
Australia	Nick LIGACS	nick.ligacs@hydro.gov.au
France	Geoffroy SCRIVE	geoffroy.scrive@shom.fr
Germany	Mathias JONAS	mathias.jonas@bsh.de
Japan	Tatsuo KOMORI	tatsuo-komori@kaiho.mlit.go.jp
Norway	Robert SANDVIK (**Vice Chair**)	robert.sandvik@ecc.no
United Kingdom	Jonathan PRITCHARD (**Chair**)	jonathan.pritchard@ukho.gov.uk
IHB	Tony PHARAOH (**Secretary**)	addt@iho.int
	Yves GUILLAM	adcs@iho.int
Expert contributors	**Name**	**E-mail**
ChartWorld	Juergen A. KUTERNOGA	ku@chartworld.com
Furuno Finland	Hannu PEIPONEN	hannu.peiponen@furuno.fi
	Antti KUKKONEN	antti.kukkonen@furuno.fi
IC-ENC	Kevin BLACK	kevin.black@ic-enc.org
IIC Technologies	Raj ALLA	rajalla@iictechnologies.com
Japan Radio Company	Takeshi TOKOI	tokoi.takeshi@jrc.co.jp
Kelvin Hughes	Martin TAYLOR	martin.s.taylor@kelvinhughes.co.uk
	Andy FROMINGS	andy.fromings@kelvinhughes.co.uk
PRIMAR	Tore HALSET	halset@ecc.no
SAM Electronics	Bernhard NOEGGERATH	bernhard.noeggerath@sam-electronics.de
	Wolfgang PIEPER	wolfgang.pieper@sam-electronics.de
Transas	Konstantin IVANOV	konstantin.ivanov@transas.com
(Contractor to AHS)	Paul BUCK	pb@madzebra.com

Annex B

IHB Report

Status of Migration to S-63 Edition 1.1

IHB - 17 August 2015

1. At its 4th meeting in September 2012, the IHO Hydrographic Services and Standards Committee (HSSC) set 1 January 2014 as the termination date for S-63 edition 1.0.

2. A limited extension was granted to two data servers who requested more time to complete the migration of a small proportion of legacy ECDIS systems to be able to use S-63 edition 1.1 ENCs.

3. The extension was granted subject to the data servers reporting to the IHB, on a quarterly basis, the progress in migrating legacy systems. The following table summarizes the evolution from 1 January 2014 to 30 June 2015.

Status as of	**1 Jan 2014**	**31 Mar 2014**	**30 Jun 2014**	**30 Sep 2014**	**31 Dec 2014**	**31 Mar 2015**	**30 Jun 2015**
Consolidated percentage of legacy users reported by the data servers	21 %	10 %	8 %	6 %	6 %	5 %	4,5 %

4. It appears that the percentage is reaching a level which might be difficult to reduce any further in the foreseeable future without any drastic action.

5. The following options are offered for the consideration of the DPSWG and the RENCs in order to advise HSSC on the way forward:

   a. No further monitoring and no action, considering that there is no major drawback to letting the remaining users continue using S-63 Ed. 1.0 until their legacy systems are removed or replaced, however long it may take;

   b. Continue monitoring the situation on a quarterly basis and postpone the consideration of any further action until HSSC-8;

   c. Continue monitoring the situation on a quarterly basis and inform the two data servers that the exemption will terminate at [date to be notified with [six-month] notice]. The date could be aligned with the end of the authorized use of S-52 Edition 6.0 and S-52 Presentation Library Edition 3.4 (expected date: 1 Sept 2016) which will require a system upgrade.

   d. Continue monitoring the situation on a quarterly basis and requests that the two data servers negotiate a termination date with each legacy user and report to the IHB within [six-months].

Annex C

Overall status of the work programme of - DPSWG

Compiled by - Jonathan Pritchard [*Chair*].

Principal goals or priorities for your group	Current or expected gaps and needs that may prevent completion of tasks on time	Any amplifying comments
Creation of edition 2.0 of S-63 for S-10x data products	Input to document creation has been difficult to obtain due to resource constraints.	A lot of input gathered over the last few DPSWG meetings has been compiled into a skeleton document which needs to be filled out. DPSWG chair has collated input from group members to date but more work is required and currently there is no detailed plan to achieve the goal of a "draft" during 2015. This situation may have changed by HSSC however. A drafting group later in 2015 is a contingency measure to try and focus group efforts on turning concepts into concrete documentation.
Support to data protection scheme administrators and end users (including ECDIS OEMs)	On track	A reactive function for the DPSWG group. A mixture of simple queries and issues of policy which are progressed with IHB staff.
Input into other IHO working groups on S-63 2.0 structure.	On track	The basic structure of the S-63 2.0 scheme and the division of responsibilities is largely defined and needs to be presented to the IHO S-100 WG along with detailed updates to existing documentation and suggestions. This will be accomplished for the next S-100WG meeting. Closer cooperation with S-100 WG has not been possible to date due to resource constraints

Annex D

DPSWG Work Plan 2016-2017

A	Maintain and extend Publication S-63
B	Provide S-63 technical and operational support to Data Servers and OEMs
C	Develop a more detailed work plan for future standards relating to Data Protection and Security of ENC data
D	Engage stakeholders in drafting of new edition of S-63 to support S-101 development
E	Support transition to latest edition of S-63 (1.1)

Work items

Work item	Title	Priority H-high M-medium L-low	Next milestone	Start Date	End Date	Status P-planned O-ongoing C-completed S-Superseded	Contact Person(s)	Related Pubs / Standard	Remarks
A	Maintain and extend Publication S-63	M	-			C	Chair		**1.1.2 completed and published**
B	Provide S-63 technical and operational support to Data Servers and OEMs	M	-			O	Chair		
C	Develop a more detailed work plan for future standards relating to Data Protection and Security of ENC data	M	Completed Plan		March 2016	O		S-100/S-101	Plan to be submitted following meeting in March 2016

Work item	Title	Priority H-high M-medium L-low	Next milestone	Start Date	End Date	Status P-planned O-ongoing C-completed S-Superseded	Contact Person(s)	Related Pubs / Standard	Remarks
D	Engage stakeholders in drafting of new edition of S-63 to support S-101 development	H	First draft for WG meeting March 2016		November 2016	O			Ongoing with industry participants and working group members. Early draft with group members and being authored.
E	Support transition to latest edition of S-63 (1.1)	L			January 2015	O			Monitoring of compliance in progress. Otherwise no other input required.

Recent Meetings

Date	Location	Activity
13-15 May 2014	IHB, Monaco	DPSWG-10
2016 (TBD – Proposed March 2016)	TBD – Proposed co-located with S-100 WG	*DPSWG-11*

Chair: Jonathan PRITCHARD
Email: jonathan.pritchard@ukho.gov.uk
Vice Chair: Robert SANDVIK
Email: robert.sandvik@ecc.no
Secretary: Tony PHARAOH
Email: addt@iho.int