WEND11-06D

11TH WEND COMMITTEE MEETING
Tokyo, 2-5 September 2008

IC-ENC Status Report

Submitted by:	International Centre for ENCs
Executive Summary:	Short report on recent activities within IC-ENC, and update on progress with actions 6 and 7 from WEND10 and actions 7 – 9 from ESF-2.
Related Documents:	WEND10-7C; X-WEND1-05E; WEND11-7A
Related Projects:	Not Applicable

1 Update on IC-ENC Activities, Progress and Concerns

The International Centre for ENCs (IC-ENC) was formed on 1st July 2002, and together with PRIMAR is one of the two RENCs operational today. IC-ENC provides independent ENC quality assurance and international distribution services on a not-for-profit basis to its members. IC-ENC operates from two offices, the headquarters in UK and a satellite RENC office in Australia (AUSRENC), who together have agreements with 28 member nations, 20 of which currently have ENC data flowing through IC-ENC appointed re-sellers to the market. Since the last WEND meeting, Brazil, Colombia, Ecuador, and New Zealand have joined IC-ENC.

The focus of IC-ENC operations remains the provision of a final and independent quality assurance process, prior to ENC release, to ensure the supply of high quality consistent data to end users. This promotes confidence in the use of ENCs and enhances the total credibility of an ENC service.

Working with such a large number of nations, each at different stages in their ENC production programmes, has demonstrated the wide range of experience and expertise that exists, and therefore the need for a central coordinating body to ensure a consistent quality standard is achieved across the whole WEND database. IC-ENC therefore supports the conclusions of the WEND Task Group, in particular the proposed new WEND Principle 2.2 (WEND11-7A refers).

Given the variability which exists, IC-ENC has recently introduced a "Partnership Programme" which allows a degree of tailoring of the quality assurance service to reflect the different and changing support needs and requirements of individual members. In addition, this programme has extended the service beyond the traditional and straightforward S-58 validation and data overlap checks to encompass a range of new data consistency and usability checks where feedback on the suitability of the product for navigational purposes is also provided. This includes viewing the product on an ECDIS and performing a variety of horizontal and vertical consistency checks.

As outlined in IC-ENC's report to the extraordinary WEND meeting last year (section 4.1 of X-WEND1-05E refers), overlapping data remains a particular concern, and makes it difficult for Data Servers to provide seamless coverage within their integrated services. Following a recent audit of the IC-ENC database, IC-ENC is now also concerned about the variability in updating across the WEND database.

WEND Principle 2.7 makes it clear that Member States are expected to ensure that "the updating of ENCs should be at least as frequent as that provided by the nation for correction of paper charting", and the mariner will expect his ENCs to be "adequate and up to date" in accordance with SOLAS V Regulation 27.

IC-ENC's audit has demonstrated that not all producing nations are managing to achieve this level of updating, with some nations having no apparent updating infrastructure in place. IC-ENC is

therefore giving greater emphasis to this issue within its quality assurance processes, and working with its members, particularly those who newly join IC-ENC, to ensure the ENC data IC-ENC distributes is properly maintained for navigationally significant information.

2 Review of Actions from WEND10, X-WEND1 and ESF2

2.1 WEND10 Action 7: *RENCs to report back to WEND on the issues raised in the paper WEND10-7C*

WEND10-7C was written to broaden the awareness and understanding of S-63 (the IHO's Data Protection standard) by providing an introductory guide to how the components of S-63 works to manage the licensing of ENC data within integrated services (copy attached at Annex A); and to emphasise the role of the 'Data Server' within the S-63 scheme, explaining how Data Servers are central to the delivery of such integrated services.

The paper pointed to several issues which Member States should consider when setting their distribution policies to take account of the flexibilities Data Servers need to be able to successfully deliver integrated services. The paper outlined how this has been made more complex by S-63 implementation problems by some ECDIS manufacturers. Since then, IMO has agreed amendments to the ECDIS Performance standards which include a requirement for ECDIS to be able to use S-63 protected ENC data. This mean that OEMs now have to implement S-63 correctly, and in full, as compliance will be tested by type approval (using IEC61174). The DPSWG has also completed work on edition 1.1 of S-63 (endorsed by CHRIS19) giving improved guidance to OEMs and providing test data sets to support IEC61174 testing. In addition IMO has issued a Safety of Navigation circular (SN.1/Circ266) emphasising the need for ECDIS s/w to be maintained in line with IHO standards. The issue of updating shipborne navigation and communication equipment is likely to be discussed further at NAV55

Finally the paper confirmed that, like other data protection schemes, S-63 includes a variety of organisations who all play a role in ensuring the successful protection of the data through the distribution chain, and who must therefore each operate as 'trusted parties'. S-63 is therefore designed to provide protection for those outside of the scheme, rather than for these 'Data Servers' and 'OEMs' (often the same organisations in both cases) who operate within the scheme under licence from the scheme administrator (IHB).

The concepts outlined in this paper, and the issues identified, remain as true today as when the paper was originally written in 2006, and Member States are therefore invited to revisit these issues when setting or reviewing their distribution policies to ensure they do not unintentionally hamper the development of integrated services.

2.2 WEND10 Action 6: *RENCs to report back to WEND on how to harmonize the various means of ENC distribution that exist between the two RENCs*

In many respects, there is already a degree of harmonisation in distribution policies between the RENCs (e.g. subscription periods, SENC delivery requirements, sales report formats). However, the main difference which remains is the approach towards supporting Data Servers.

The policy of IC-ENC members is to allow a number of competent organisations to operate as Data Servers, and so each deliver their own branded ENC services. Before appointment, these organisations must successfully complete IC-ENC's required technical compliance tests to demonstrate their competence to deliver a reliable integrated service where the integrity of the ENC data is suitably assured, and the data is properly protected through the correct implementation of S-63.

The integrity of ENC data within these integrated services can then be easily confirmed by checking the CRCs provided by the originating Hydrographic Office against those found in the CATALOG.031 on the service media provided by a Data Server. Before loading any data, the

ECDIS will also compare these same CRC values quoted in the CATALOG.031 files against the calculated CRC value of the ENC data it has just decrypted, and so protect the user from any accidental corruption which may have occurred.
On the other hand, the policy of PRIMAR members is to assign the Data Server role exclusively to the RENC which therefore manages the encryption and authentication of ENC data centrally, and provision of this data within a single integrated service through a network of distributors. In light of this, PRIMAR has developed a comprehensive service delivery infrastructure in support of this integrated service.

This difference in approach points to the ongoing discussion about where the boundary of government responsibility lies, and the role of competition in the delivery of ENC services. This fundamentally dictates the scope of RENC operations and distribution policies. It is recognised that both can be argued to be valid approaches having their own strengths and weaknesses. However, the two models are incompatible and this has frustrated attempts to implement reciprocal RENC data exchange as envisaged by WEND.

IC-ENC reported to the extraordinary WEND meeting last year (section 3 of X-WEND1-05E refers) that the relevant experts of both RENCs have met on several occasions in order to confirm the current policies of each RENC in this regard, and to identify the issues which arise from these differences in approach. Further discussions are now ongoing between the operators of both RENCs to identify the relative strengths and weaknesses of each model in order to work towards a common solution which meets the needs of the mariner.

To this end, the RENC operators have re-affirmed their joint commitment to further cooperation between the two RENCs. They recognise that the operational models and policies of the two RENCs need to be more closely aligned in order to gain efficiencies of operation and to optimize the quality and consistency of all ENC data. There is also agreement that the operating environment should favour the development of integrated services and that the integrity of the original ENC data has to be ensured through the distribution chain to the end-user.

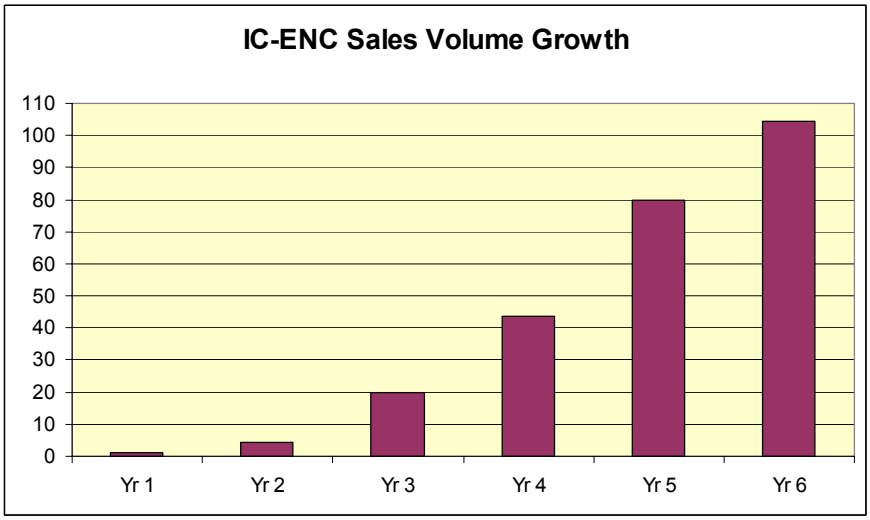
2.3 ESF-2 Action 7: *The two RENCs to conduct a study of the level of ENC use onboard SOLAS vessels and report back to WEND on the findings*

IC-ENC responded to this action by providing a brief analysis of the sales trends experienced within IC-ENC to the extraordinary WEND meeting last year (section 4.3 of X-WEND1-05E refers).

At the time, IC-ENC estimated that there were around 2,000 registered ENC subscribers using IC-ENC data, with approximately 60% accounted for by government backed customers (e.g. navies, coastguards, pilots, etc.) and shore based customers (e.g. training schools). Therefore only about 40% of registered ENC users are from SOLAS regulated shipping, and approximately 80% of these are accounted for by the particularly safety conscious tanker and passenger ship segments of the market.

IC-ENC also reported that sales were heavily weighted to coverage within Europe, with IC-ENC members outside Europe seeing a much lower uptake. The report also identified a worryingly high level of customer churn (i.e. customers who fail to renew their subscriptions), with product quality and price cited as the most likely cause of this trend.

In the last year, IC-ENC members have lowered their wholesale prices significantly, such that the average wholesale price of IC-ENC data sold in 2008 is now 40% less than it was in 2007. Overall turnover has continued to grow, and is now more than 100x higher than it was when IC-ENC formed in 2002, as shown in the graph below.



Despite this steady growth, once the equivalent growth in the IC-ENC database is taken into account, the average sales per available ENC unit has remained relatively static since 2006. However, IC-ENC has noted a particularly strong growth in sales since the start of 2008 and this has finally halted this trend and we are now starting to see a genuine expansion in the uptake of ENC users within the SOLAS regulated shipping.

Even so, this still remains a very small percentage of the SOLAS market (<5%), and only a modest percentage of those ships thought to have a suitable ECDIS installed. Furthermore the sales pattern shows that the dominance in sales of European coverage has remained, but this is now expected to weaken as contiguous ENC coverage grows along major trading routes.

With improvements in coverage, falling wholesale prices and the positive outcome of NAV54, there is a renewed interest in ECDIS and IC-ENC expects a significant change in sales patterns over the coming few years.

2.4 ESF-2 Action 8: *Licensing bodies to examine alternative licensing conditions and arrangements with a goal toward more flexibility and report back to WEND*

Since the last WEND, IC-ENC has both reduced its overall wholesale prices, and relaxed the business terms with its appointed Value Added Resellers (VARs) to provide them with greater flexibility when handling multi-user licences.

IC-ENC has recently conducted a survey of its VARs to gain feedback on a variety of pricing and licensing issues. The conclusions of this feedback suggest that current IC-ENC business terms generally provide our VARs with sufficient flexibility to provide the types of integrated services they wish to offer their SOLAS customers. In light of this feedback, the IC-ENC Steering Committee will be considering some further minor changes to its business terms when it meets following WEND, particularly with respect to subscription periods and the option to harmonise with PRIMAR on pricing cells rather than units.

2.5 ESF-2 Action 9: *Licensing bodies to review and report back to WEND their current information requirements for maintaining privacy*

The contract IC-ENC has with its appointed VARs recognises the need to keep confidential any marketing, sales or financial information which is supplied between the parties, unless this is already in the public domain. IC-ENC therefore does not provide details of customer or sales patterns linked to particular VARs.

IC-ENC VARs are required to confirm the total volume of sales of specific ENC units for invoicing purposes. They do not have to provide customer information. However, IC-ENC

recognises that its appointed VARs also purchase ENC data from PRIMAR who require details of each customer that is licensed, and for this information to be submitted via an XML based report. In order to harmonise reporting requirements, and so allow VARs to only have to support a single report format, IC-ENC therefore allows VARs to submit reports in the same XML format.

Most VARs now report in this XML format, and all VARs have confirmed they are happy to report in this format going forward. IC-ENC is therefore considering moving to establishing this as its standard report format as well.

3 Action Required of WEND

The WEND Committee is invited to note:

- IC-ENC concerns regarding overlapping data and ENC updating regimes
- The introductory guide to S-63 attached at Annex A, and the issues to consider when setting distribution policies outlined in WEND10-7C
- The ongoing work and commitment by the two RENC operators to identify the best way to harmonise RENC operations, and that a common interpretation within the WEND Committee of governmental responsibility in relation to ENC service provision would assist in this.

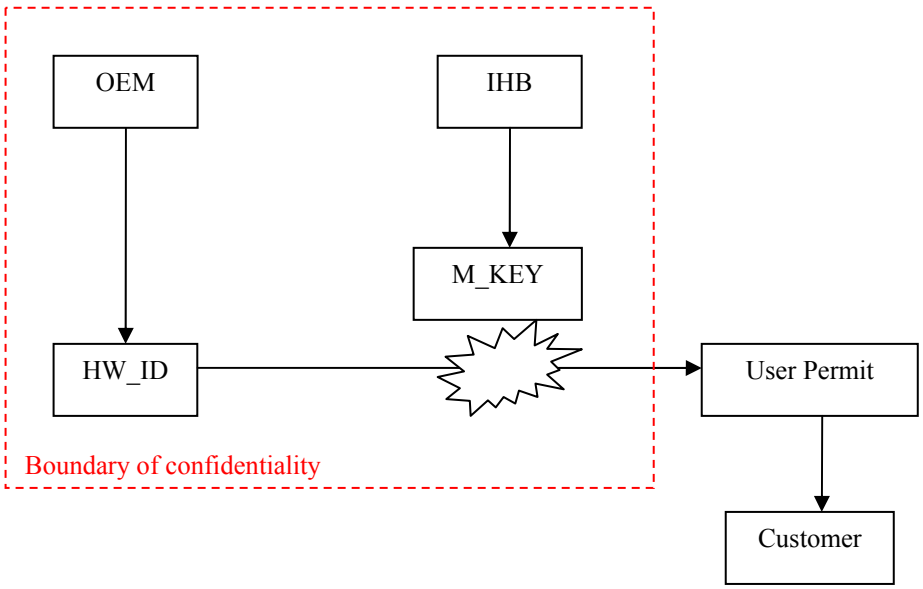
ANNEX A

S-63 Encryption – The Basics

The ECDIS Dimension

When a customer buys an S-63 compatible ECDIS, he will be given a "**User Permit**". This User Permit is an encrypted version of the "**Hardware Identifier**" (HW_ID), a unique number which the Manufacturer defines for each ECDIS it makes.

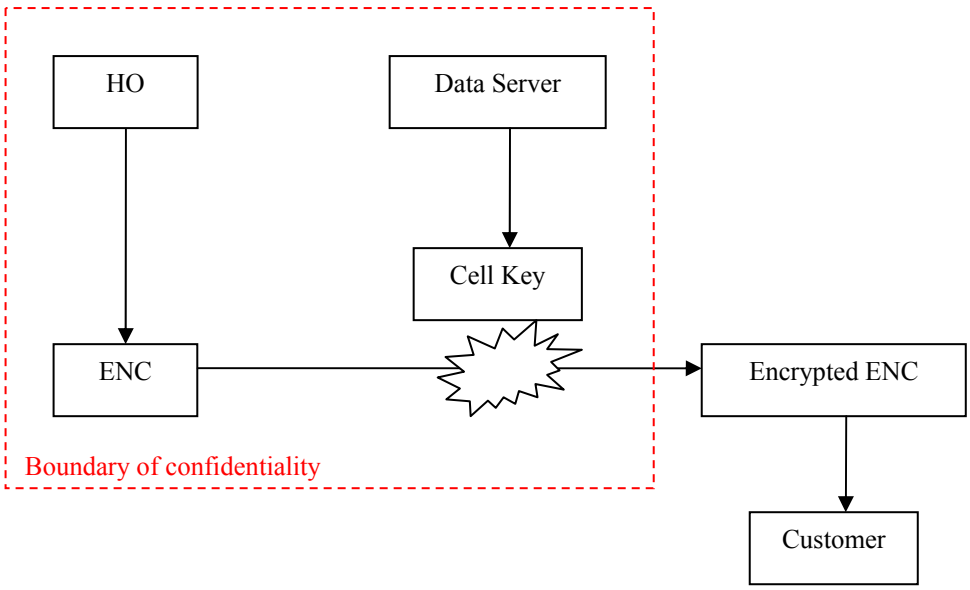
The HW_ID is encrypted using a "**Manufacturer Key**" (M_KEY), a unique number given to the Manufacturer by the Scheme Administrator (i.e. IHB). The user of the ECDIS therefore never knows the HW_ID or the M_KEY which are both confidential pieces of information within the scheme.



Data Servers are provided with details of all of the M_KEY values by the IHB when they are registered. When a Data Server licences a new customer who has ordered ENCs, the customer is asked to provide the User Permit. Since the Data Server already knows the M_KEY used to create this User Permit, the Data Server is able to calculate the HW_ID of the system used by his customer.

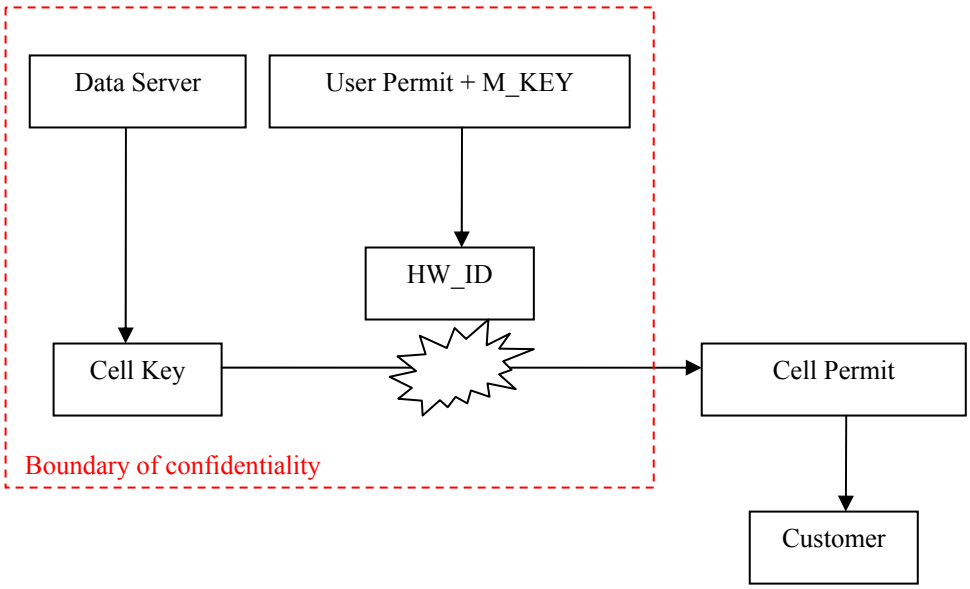
The ENC Dimension

The Data Server will have already encrypted the ENCs in its database using a series of "**Cell Keys**". The Data Server may define these Cell Keys itself, or they may be supplied by the HO or RENC, and each Cell Key should be unique to a specific ENC cell.



The Customer Dimension

For a customer to be able to load and use an encrypted ENC onto his ECDIS, he needs a "**Cell Permit**" which decrypts the data within the ECDIS. This Cell Permit is an encrypted version of the Cell Key, and is encrypted using the HW_ID. This means that the Cell Permit only works to decrypt a particular ENC cell on a particular ECDIS system. The Cell Permit also contains an expiry date to control how long the customer can continue to apply updates, thus defining a subscription period.



The ENC ordering process

1. When a customer places an order for ENCs, he provides the Data Server with the User Permit for his ECDIS, which he received from the manufacturer when he purchased the ECDIS.
2. The Data Server decrypts the User Permit, using the M_KEY specific to the manufacturer of the ECDIS, to derive the HW_ID.

3. The Data Server then encrypts the Cell Key(s) for the particular ENC(s) being ordered, using the customer's HW_ID which has been derived in step 2, to create the Cell Permit(s), which the Data Server then provides to the customer.
4. The customer loads these Cell Permits into his ECDIS which then decrypts them using the HW_ID which is stored securely in the ECDIS to derive the Cell Keys.
5. The customer loads the encrypted ENC data into his ECDIS which then applies the relevant Cell Key against the relevant encrypted ENC cell to decrypt it, convert it into SENC and store it ready for display. Under the confidentiality agreement with the IHB, the ECDIS manufacturer must ensure that the SENC file is stored safely so that the customer cannot easily access it, and so that the decrypted ENC data before it is converted into SENC is also not easily accessed or stored.

S-63 Encryption – Who Knows What

The HW_ID, M_KEY and Cell Key are all confidential information that control the encryption / decryption process. Knowledge of this information is therefore managed under confidentiality agreements with IHB (different versions for manufacturers and Data Servers) as follows:

	Manufacturer	Data Server	Customer
HW_ID	Yes, generates them	No, but can derive it with User Permit	No
M_KEY	Yes, but only their own provided by IHB	Yes, all of them provided by IHB	No
User Permit	Yes, generates them	Yes, gets them from customer	Yes, gets them from manufacturer
Cell Key	No	Yes, generates them, but only knows their own unless "unicity" is observed with other Data Servers	No
Cell Permit	No, but can order them from a Data Server	Yes, generates them	Yes, gets them from Data Server

The S-63 Trusted Circle

As both Manufacturers and Data Servers have access to this confidential information, and in some instances are creators of it, they are in a responsible position and so must be trusted by the owners of the data which S-63 is supposed to protect. Thus S-63 protects against misuse by customers, but not against misuse by manufacturers or Data Servers.

To illustrate this, if a manufacturer receives encrypted data he obviously does not have the Cell Keys, and so in theory cannot decrypt the data. However, the OEM has developed a display system which is capable of decrypting this data. Therefore, all the OEM has to do is to order Cell Permits from a Data Server. Since the manufacturer already knows the HW_ID used by the Data Server to encrypt the Cell Permit, he can decrypt this Cell Permit and thus derive the Cell Keys. He is then able to decrypt the data for whatever purpose.

Thus, withholding cell keys or denying access to non-encrypted data to a manufacturer makes little sense. If the manufacturer really wanted to access the non-encrypted data, he only has to acquire Cell Permits from a Data Server. Since most Data Servers provide free R&D licences to manufacturers to help them develop their system compatibility with the Data Server's own service, this is typically already available to them anyway.

Similarly, if a Data Server (acting as a distributor) receives encrypted data from a supplier, he also does not have the Cell Keys and so in theory cannot decrypt the data and cannot generate Cell Permits for his customers. Therefore, the Data Server must order these Cell Permits from his supplier in order to satisfy his customer's order. In doing so he will need to provide his supplier with the customer's User Permit as well.

The Data Server will therefore be able to derive the customer's HW_ID from this User Permit because the Data Server already knows the M_KEY. And, as soon as he receives the Cell Permits from his supplier, he will be able to use the HW_ID to decrypt these Cell Permits and so derive the Cell Keys.

From this, he can then decrypt the data himself. Thus, withholding cell keys or denying access to non-encrypted data to a Data Server makes little sense as well.

Customers cannot do any of this since they do not know the HW_ID or M_KEY values. If they wish access to the non-encrypted data, they will either have to crack these keys (plus read up on how S-63 works), or to reverse engineer the ECDIS to get at the data stored therein.