ESTA CIRCULAR REQUIERE SU VOTO

Dossier del BHI No. S3/8151/CHRIS

CIRCULAR No. 38/2000
5 de Septiembre del 2000

ESQUEMA(S) DE SEGURIDAD DE LAS ENCs

Ref.: Circular del BHI No. 40/1999 fechada el 27 de Agosto de 1999

Muy Señor nuestro,

Se atrae la atención de los Estados Miembros sobre la Circular No. 40/1999, que trata sobre el tema arriba indicado. Desde la edición de esta Circular, varios Estados Miembros han expresado su preocupación por la entrega de sus datos sin seguridad. Esto se ha reflejado en informes nacionales durante las anteriores reuniones de CHRIS y WEND, pe de Australia, India, Malasia y Rusia, según lo contenido en el Documento WEND/5/6A, disponible en el sitio Web de la OHI (www.iho.shom.fr - Estados Miembros únicamente). Se han recibido solicitudes adicionales de la industria solicitando una aclaración sobre el pretendido informe de la OHI sobre la codificación de datos ENC.

El tema del (los) esquema(s) de seguridad fue tratado en la 11ª Reunión de CHRIS, en Noviembre de 1999, y posteriormente en la 5ª Reunión de WEND, en Marzo del 2000. En la reunión de CHRIS, la mayoría consideró que era deseable la codificación. Se convino además que, si se introdujera la codificación, debería normalizarse y que, finalmente, la OHI tendrá que definir su postura en este asunto, y deberá adoptarse una política antes de que puedan decidirse los detalles (ver Circular del BHI No. 3/2000). En la reunión de WEND, el RENC Europeo PRIMAR indicó que el esquema de seguridad que estaban usando (pe un algoritmo de codificación conocido como ”BLOWFISH” y varios protocolos de codificación del propietario) estarían disponibles públicamente para aquellos SHs que deseen adoptar su esquema (ver Circular del BHI No.23/2000).

El esquema de seguridad utilizado por PRIMAR, principalmente previsto para proporcionar la autenticación de los datos y para proteger los datos ENC de copia, uso o cambio no autorizados, se describe en el Anexo A. En particular, se atrae la atención sobre el párrafo 5.3, que explica detalladamente un posible método según el cual la OHI podría asumir la responsabilidad del esquema y del párrafo 4, que proporciona detalles sobre cómo utilizar realmente este esquema de seguridad.

Se ha indicado que el Esquema de Seguridad de PRIMAR está siendo implementado actualmente o está siendo desarrollado por más de 10 fabricantes de ECDIS o ECS.

Se solicita pues a los Estados Miembros que respondan al cuestionario adjunto como Anexo B **antes del 15 de Octubre del 2000** y que indiquen, por votación, si debería haber un sistema de codificación específico recomendado por la OHI.

En nombre del Comité Directivo
Atentamente,

Contralmirante Neil GUY
Director

Anexos: Anexo A: Esbozo del Esquema de Seguridad de PRIMAR;
Anexo B: Cuestionario / Papeleta de Voto.

Anexo A a la Circular
del BHI No. 38/2000

PRIMAR™
OFFICIAL ENC SERVICE

Esbozo del Esquema de Seguridad

ECC
ELECTRONIC CHART CENTRE

1. Introducción

PRIMAR es el primer Centro Regional operativo del Mundo, de Servicios de Cartas Electrónicas de Navegación (ENC) conformes al modelo WEND de la OHI. El Servicio PRIMAR consiste en el suministro de ENCs oficiales con actualizaciones disponibles 24 horas al día globalmente, on-line o en CD-ROM.

PRIMAR está manejado por el Servicio Hidrográfico del RU y por el Centro AS de Cartas Electrónicas (ECC). El ECC es el operador y promotor de los sistemas y servicios que permiten a PRIMAR ofrecer sus servicios globales.

Este documento describe parte de la información de antecedentes requerida para comprender porqué PRIMAR y el ECC han desarrollado el esquema de seguridad y ofrecen su experiencia derivada de su práctica. Explica los procesos que conducen al desarrollo del esquema de seguridad y las interacciones con los utilizadores y los productores del sistema. Se proporciona también una visión de conjunto no técnica del esquema de seguridad.

El ECC y PRIMAR describirán también el tipo de apoyo que pueden proporcionar como solución provisional hasta que la OHI haya asumido completamente las responsabilidades asociadas al esquema de seguridad.

2. Desarrollo del Esquema de Seguridad utilizado por PRIMAR

PRIMAR es el operador del RENC en Europa, con la cooperación de muchos Servicios Hidrográficos (SHs) en Europa y en el mundo entero. PRIMAR proporciona actualmente un servicio comercial y global desde el principio hasta el final, distribuyendo ENCs oficiales en CD y un servicio on-line disponible 24 horas al día.

Algunos de los SHs indicaron claramente, cuando empezó el trabajo de desarrollo del servicio en PRIMAR, que sus intereses comerciales tenían que ser protegidos de modo que no pudiesen ser utilizados de forma errónea o copiados ilegalmente. Algunos SHs del mundo entero ya habían informado sobre problemas de la puesta en el mercado de productos de cartografía digital no garantizados en el mercado. Los requerimientos básicos de los SHs fueron que:

- El esquema debe proteger su interés comercial;

- El esquema debe incluir:

  - La autenticación mediante Firmas Digitales;
  - El Acceso Selectivo mediante una Administración de Códigos;
  - La Protección contra la Piratería mediante la Codificación;
  - La Integridad de Datos y Servicios.

Desarrollar un esquema de seguridad implica también una amplia comunicación y discusiones técnicas con los representantes de la industria. Los argumentos clave del ECDIS, del ECS y de la industria OEM para un esquema de seguridad fueron:

- El esquema debe basarse en normas internacionales, o utilizar las normas de la industria;
- El esquema debe ser diseñado de modo que pueda ser utilizado para contener también otros tipos de productos hidrográficos digitales;
- El esquema debe ser normalizado en la Comunidad Hidrográfica Internacional, de modo que todos trabajen con una norma global uniforme;
- Facilidad de implementación, uso operativo y administración del esquema de seguridad.

Esta información constituyó algunos de los requerimientos del utilizador, utilizados para diseñar el esquema de seguridad. Se combinó con las experiencias del ECC, obtenidas a partir del proyecto ECHO, financiado por la Comisión Europea, y a partir de un largo trabajo y experiencias acumuladas en el SH del RU, como parte del suministro de su servicio ARCS.

Siguió un largo período de evaluación de las normas internacionales de seguridad, de diseño del esquema de seguridad y de su revisión con los representantes de la industria. La información proporcionada por la industria y las experiencias del desarrollo interno dieron como resultado cambios, ajustes y mejoras. Se utilizaron amplios recursos para informar a la industria acerca de las intenciones de PRIMAR de adoptar el esquema de seguridad y de ayudar en el desarrollo de un apoyo para el esquema. Una consecuencia fue el suministro de más aclaraciones y de un código original de muestra, junto con un seguimiento más estrecho. Fue necesario que PRIMAR cambiase su actitud, para informar a la industria sobre los nuevos servicios garantizados. Al mismo tiempo, varios de ellos estaban pasando pruebas de sanción de prototipos de ECDIS en sociedades de clasificación. Al ECC y a PRIMAR les ha llevado de 15 a 18 meses desarrollar el esquema de seguridad, introducirlo en la industria y ponerlo en funcionamiento comercialmente.

3. Construcción del Esquema de Seguridad

Esta sección presentará brevemente todas las construcciones definidas en el esquema de seguridad y cómo se utiliza para operar el esquema con la seguridad adecuada. Hay más información sobre el esquema de seguridad disponible en el ECC AS (www.ecc.as). La documentación del sistema de seguridad utiliza conceptos de seguridad reconocidos internacionalmente y normas que se han descrito con una definición de los procedimientos apropiados para un funcionamiento logrado.

3.1 Certificado Digital

Un certificado es un documento firmado electrónicamente, que vincula estrechamente la clave pública a la identidad de una parte. Su objetivo es impedir a alguien que se haga pasar por otra persona. Si un certificado está presente, el receptor (o un tercero) puede comprobar que la clave pública pertenece a una parte nombrada. Se utiliza la clave pública almacenada en el certificado digital para comprobar la firma digital.

El esquema de seguridad de PRIMAR utiliza certificados digitales basados en la norma internacional CCITT X.509 "El Directorio – Estructura de Autenticación".

3.2 Firma Digital

La Autenticación es todo proceso a través del cual una persona confirma y comprueba cierta información. A veces se puede querer comprobar, pe el origen de un documento, la identidad del emisor, la hora y la fecha en que ha sido enviado y/o firmado un documento o la identidad del utilizador. Una *firma digital* es un medio criptográfico mediante el cual muchos de estos documentos pueden ser comprobados. La firma digital de una ENC es un fragmento de información que vincula la ENC al RENC/SH productor mediante la combinación de la clave privada/pública del SH/RENC, que se obtiene a partir del certificado digital, ref. 3.1.

La autenticación es todo lo que se hace para asegurarse de que un intruso no pueda alterar, falsificar una ENC, y para garantizar que procede de un SH/RENC aprobado.

El esquema de seguridad utiliza firmas digitales basadas en la norma internacional "Digital Signature Standard (DSS)" FIPS Pub 186. Cada archivo ENC tiene una única firma digital que asegura los orígenes del archivo.

3.3 Codificación (Protección contra la Piratería) y Acceso Selectivo

El esquema de seguridad utiliza la codificación para proporcionar protección contra la piratería. El algoritmo de codificación "Blowfish" ha sido seleccionado a causa de su fuerza y, como no está patentado, puede ser exportado y utilizado gratuitamente. Como PRIMAR está utilizando un volumen de clave de 40-bits, puede ser exportado al mundo entero sin ninguna restricción. (El algoritmo soporta volúmenes de clave de hasta 448-bits, pendientes de las aprobaciones para la exportación).

El esquema codifica sólo los ficheros ENC (células básicas y actualizaciones). Cada ENC (una célula) será codificada utilizando una Clave de Célula diferente. Además, cada edición de una ENC será codificada con una Clave de Célula diferente. La misma Clave de Célula será utilizada para codificar todas las actualizaciones publicadas para esa edición de la ENC.

El esquema codificará la totalidad del contenido de los ficheros de datos. Esto se aplica a los ficheros de células básicas y de actualizaciones. Los ficheros codificados serán conformes al convenio sobre Especificación de Productos ENC en la norma S-57.

El Acceso Selectivo es la capacidad de almacenar grandes cantidades de ENCs, p.e. en un CD-ROM, y de permitir a un utilizador acceder únicamente a las células que le interesan. Se lleva a cabo codificando cada ENC con una clave diferente y permite al utilizador usar claves sólo para las células que le interesan.

3.4 Compresión

Un archivo ENC contendrá, a causa de su estructura, modelos periódicos de información, p.e. pequeñas variaciones en la información de coordenadas. El Criptoanálisis muestra que es más fácil destruir un fichero codificado que contiene secciones periódicas de información. Comprimir un fichero ENC antes de la codificación producirá un contenido completamente aleatorio y eliminará todo modelo periódico de información. El uso de la compresión se define sólo en el contexto del esquema de seguridad y no está reñido con la norma de transferencia S-57. El esquema usa el programa ZIP. La industria ha aceptado el uso de la compresión como medio de reducir también los tamaños de los ficheros.

3.5 Permiso del Utilizador

Cada utilizador autorizado de datos codificados tendrá una única identificación de hardware (HW_ID), incorporada en su sistema. El utilizador no la conoce, pero el proveedor del sistema del utilizador le proporcionará un Permiso de Utilizador, que es una versión codificada del HW_ID, que utiliza una clave y una identificación del fabricante/OEM (M_KEY y M_ID), suministrada por el Administrador del Esquema, ref. 4.1. El utilizador proporciona su Permiso de Utilizador al suministrador de servicios ENC, que producirá los Permisos de Cartas adecuados para obtener el acceso a nueva información.

3.6 Permiso de Cartas

Cada célula de ENC está codificada por el productor de datos, utilizando una Clave de Célula que es única para la célula ENC, ref. 3.3. El utilizador necesitará esta Clave de Célula para poder descodificar los datos. Se proporciona al utilizador la Clave de la Célula en una forma codificada conocida como Permiso de Cartas. La Clave de la Célula está codificada utilizando el HW_ID del utilizador a partir del Permiso del Utilizador. Asegura que un Permiso de Cartas puede ser descodificado sólo por el sistema del utilizador-final apropiado.

4. Roles y Responsabilidades del Esquema de Seguridad

Esta sección describe en términos generales los procesos y las interacciones entre los operadores de la cadena de valores de la ENC, para administrar y manejar con éxito el esquema de seguridad. El esquema adjunto se basa en el concepto WEND de la OHI, para una cooperación global en la producción y distribución de ENCs. El flujo de los royalties no está representado, ya que no forma parte del esquema de seguridad sino más bien de un acuerdo bilateral entre un SH y un RENC. Una explicación completa del esquema de seguridad está disponible en el ECC AS (www.ecc.as).

1. Todos los operadores del esquema de seguridad solicitan al Administrador del Sistema una clave y una identificación del fabricante/OEM (M_KEY y M_ID). El Administrador del Esquema mantiene un registro de todas las combinaciones válidas de M_KEY y M_ID. El Administrador del Esquema es también responsable de difundir a todos los participantes toda la otra información requerida para manejar el esquema. Incluye el mantenimiento de toda la documentación del esquema. El ECC AS opera actualmente en el RENC Europeo como Administrador del Esquema, en nombre de PRIMAR.
2. El SH puede proporcionar al RENC ENCs codificadas, los certificados digitales correspondientes y los Permisos de Utilizador, si tiene los instrumentos y la funcionalidad necesarios. PRIMAR está recibiendo actualmente ENCs decodificadas de todos los SHs cooperadores y codifica y firma todas las ENC sin cargo, en su nombre, como parte de la entrega de su servicio ENC.
3. El fabricante/OEM atribuye una identificación de hardware (HW_ID) a todos los sistemas instalados. La concatenación de la M_KEY y la HW_ID asegura que todos los sistemas instalados y los utilizadores serán identificados especialmente en el esquema. El programa del fabricante/OEM tiene la funcionalidad de generar el Permiso de Utilizador apropiado (codificando el HW_ID instalado, mediante la M_KEY como clave de codificación).
4. El Distribuidor o Agente registrará un Permiso de Utilizador de un utilizador, con el esquema para activar los servicios ENC.
5. El utilizador proporciona su Permiso de Utilizador con un pedido de nuevas ENCs a través de Distribuidores o Agentes al RENC, que generarán los Permisos de Cartas adecuados, conteniendo las claves de decodificación apropiadas para el acceso a nueva información de ENCs.
6. El RENC registrará la orden de transacción y extraerá el único HW_ID del Permiso de Utilizador. El RENC codificará las Claves de Célula ENC con los HW_ID de los utilizadores. (Esto asegura que sólo el utilizador - final apropiado podrá extraer las Claves de Células). Las Claves de Células codificadas serán entregadas como Permiso de Cartas al utilizador, con otra información aplicable.
7. El sistema del utilizador - final comprueba el certificado y la firma digital. El sistema extraerá las claves de células a partir del Permiso de Cartas, utilizando el HW_ID y decodificará las células ENC y las actualizaciones correspondientes.

Una descripción completa de los roles, responsabilidades y procedimientos para todos los operadores del esquema está definida en la documentación del esquema de seguridad.

5. Situación y Transferencia del Esquema de Seguridad a la OHI

5.1 Situación del Esquema de Seguridad

PRIMAR ha recibido la confirmación de un número sustancioso de fabricantes de ECDIS de todo el mundo, de que ya apoyan o que apoyarán el esquema de seguridad a partir de Otoño del 2000. Algunos fabricantes del sistema ECDIS han obtenido también la aprobación de su ECDIS tipo en la "Bundesamt für Seeschiffahrt und Hydrographie (BSH)" utilizando el esquema de seguridad y las conexiones on-line a los servicios PRIMAR. PRIMAR está experimentando también un interés

creciente por parte de los fabricantes de equipo ECS, que desarrollarán también apoyo para el esquema de seguridad, paralelamente con la creciente cobertura ENC.

PRIMAR ha sido contactado también por fabricantes de programas para SIGs, que han mostrado interés en desarrollar un apoyo para el esquema de seguridad, como parte de sus instrumentos de producción si se convierte en una norma global de la OHI.

5.2 Documentación del Esquema de Seguridad

El ECC AS ha desarrollado una extensa colección de documentación disponible como parte del esquema de seguridad. Incluye:

- La Interfase de Seguridad v.1.2 (Documentación del Esquema);
- Datos de pruebas, conteniendo tanto datos codificados como los datos ENC correspondientes no codificados. También incluye parámetros de pruebas específicos, utilizados principalmente por organizaciones que desarrollan apoyo para el esquema de seguridad.
- Código de muestreo original en C/Java, para demostrar cómo pueden implementarse algunos elementos del esquema de seguridad.

La documentación en su forma actual está escrita principalmente para apoyar a toda persona que desarrolle apoyo para el esquema de seguridad que decodificará información de ENCs. Pero, como los procesos son simétricos, la codificación se lleva a cabo aplicando los procesos inversos.

5.3 Transferencia de los Derechos de Autor y apoyo a la OHI

El ECC AS tiene actualmente los derechos de autor del esquema de seguridad, puesto que está siendo utilizado comercialmente por PRIMAR para proporcionar su servicio ENC. Si hay un interés en la comunidad hidrográfica para apoyar el esquema y convertirlo en una norma global de la OHI, el ECC AS transferirá los derechos de autor a la OHI. La OHI asumirá la responsabilidad de mantener la documentación y los derechos de autor, y será responsable de difundir la documentación.

El ECC AS puede proporcionar asistencia como solución provisional para la OHI, manteniendo la documentación y/o participando en todo grupo de trabajo controlado por la OHI, al que se le haya atribuido la tarea de mantener el esquema de seguridad.

Si la OHI decide utilizar los conceptos para garantizar también otros tipos de productos digitales, la documentación deberá ser ligeramente modificada, para describir cómo la construcción de la seguridad será utilizada específicamente para el producto digital, pe nombrando convenciones.

El ECC AS ha desarrollado todos los programas y procedimientos para operar como administrador del esquema en el servicio de ENCs proporcionado por PRIMAR. El ECC AS amplía esta oferta a la OHI, si decide adoptar el esquema de seguridad. Lo ideal sería que la OHI o cualquier otra persona designada por la OHI pudiese operar como administrador del esquema.

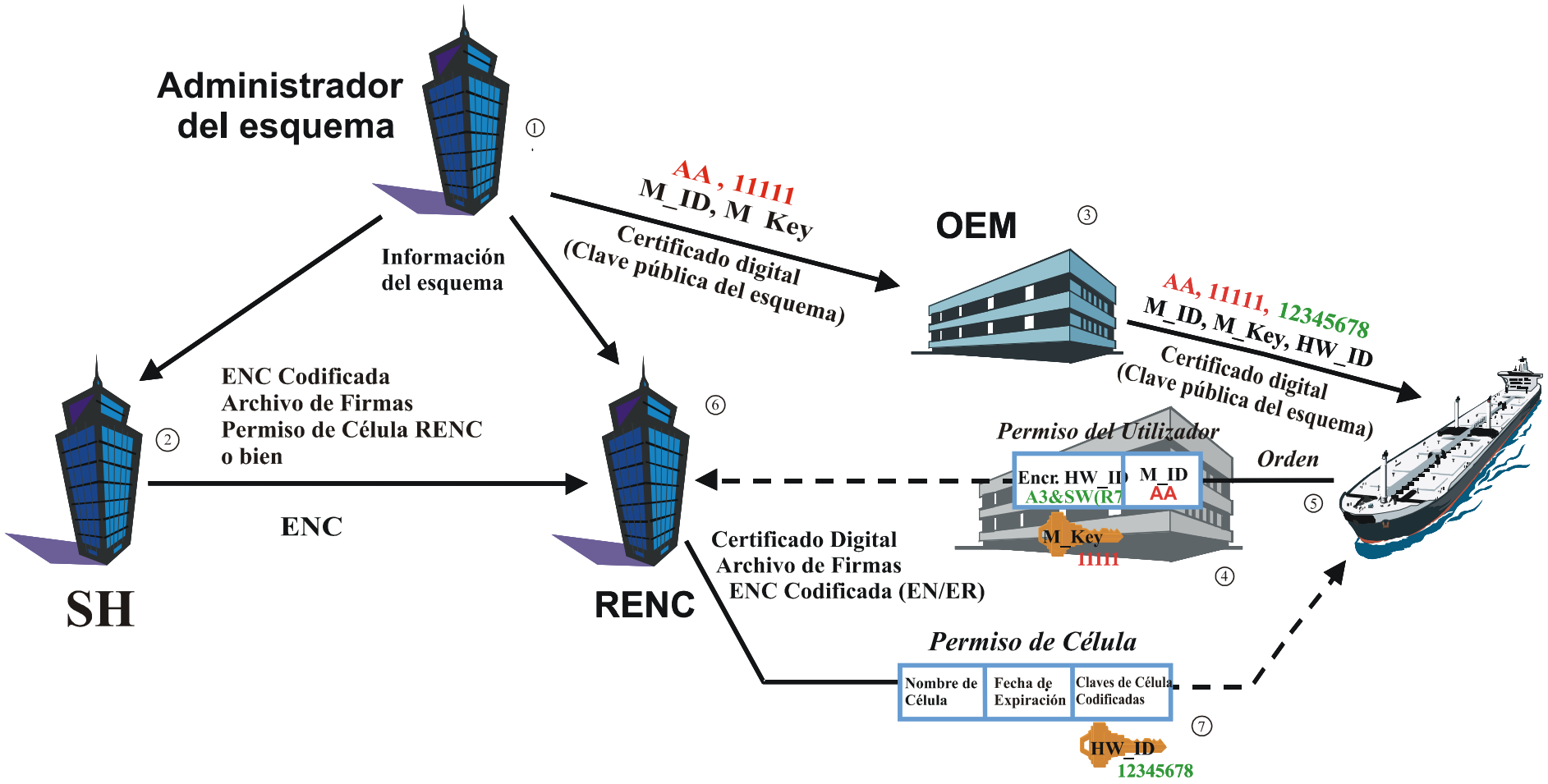
Si la comunidad de la OHI decide no adoptar un esquema de seguridad o selecciona un esquema completamente diferente del utilizado por PRIMAR, los derechos de autor permanecerán en el ECC para coordinar los servicios ENC comerciales entregados por PRIMAR. Sin embargo, PRIMAR trabajará en todas las normas que adopte la OHI sobre la seguridad. El ECC estará interesado en establecer la colaboración con otras organizaciones que planeen utilizar la seguridad para entregar un servicio ENC que permita trabajar en la normalización global.

_____

ACRONIMOS

ARCS	Servicio de Cartas Ráster del Almirantazgo (*Admiralty Raster Chart Service)* (Reino Unido)
BSH	Servicio de Navegación e Hidrografía (*Bundesamt für Seechiffahrt und Hydrographie)* (Alemania).
CCITT	Comité Consultivo Internacional de Telégrafos y Teléfonos *(International Telegraph and Telephone Consultative Committee)*
CD-ROM	Compact Disk Read Only Memory.
ECC	Centro de Cartas Electrónicas *(Electronic Chart Centre)* (Noruega)
ECDIS	Sistemas de Información y Presentación de Cartas Electrónicas *(Electronic Chart Display and Information Systems).*
ECHO	Organización Europea de Centros de Cartas *(European Chart Hub Organization).*
ENC	Carta Electrónica de Navegación *(Electronic Navigational Chart).*
ECS	Sistema de Cartas Electrónicas *(Electronic Chart System).*
FIPS	Norma Federal de Procesado de *Información (Federal Information Processing Standard)* (EE.UU.)
SIG	Sistema de Información Geográfica *(Geographic Information System) (GIS).*
SH	Servicio Hidrográfico *(Hydrographic Office) (HO)*
HW_ID	Identificación del Hardware *(HardWare Identification*)
OHI	Organización Hidrográfica Internacional *(International Hydrographic Organization) (IHO)*
M_ID	Identificación del Fabricante *(Manufacturer Identification)*
M_KEY	Clave del Fabricante *(Manufacturer KEY)*
OEM	Fabricante de Equipo Original *(Original Equipment Manufacturer)*
RENC	Centro Regional Coordinador de ENCs *(Regional ENC Coordinating Centre)*
S-57	Publicación Especial No. 57: Norma de Transferencia de la OHI para Datos Hidrográficos Digitales *(Special Publication No. 57 : IHO Transfer Standard for Digital Hydrographic Data).*
SH del RU	Servicio Hidrográfico del Reino Unido *(United Kingdom Hydrographic Office) (UKHO)*
WEND	Base Mundial de Datos de Cartas Electrónicas de Navegación *(Worldwide Electronic Navigational Chart Database).*

_____



Los números rodeados por un círculo se refieren al texto del capítulo 4.

Anexo B de la Circular
del BHI No. 38./2000

ESQUEMA(S) DE SEGURIDAD DE LAS ENCs

CUESTIONARIO / PAPELETA DE VOTO

1) ¿Tiene la intención de que sus datos ENC le sean proporcionados en formato codificado, pe directamente o a través de un RENC?

☐ SI ☐ NO

2) Si la respuesta a la pregunta 1) es "SI", ¿está de acuerdo en que debería haber un Esquema de Seguridad Recomendado por la OHI?

☐ SI ☐ NO

3) Si la respuesta a las preguntas 1) y 2) es "SI", ¿está de acuerdo en que el Esquema de Seguridad utilizado actualmente por PRIMAR, según lo descrito en el Anexo A, deberá convertirse en el Esquema de Seguridad Recomendado por la OHI?

☐ SI ☐ NO

Comentarios: ……

……

……

……

……