ỦY BAN THỦY ĐẠC VIỆT NAM
VĂN PHÒNG

LƯỢC ĐỒ BẢO MẬT DỮ LIỆU HẢI ĐỒ ĐIỆN TỬ

(Tài liệu sử dụng nội bộ)

Phiên bản 1.1.1
Tháng 4 năm 2012

Biên dịch từ tài liệu
CỤC THỦY ĐẠC QUỐC TẾ
VĂN PHÒNG MONACO

LỜI NÓI ĐẦU

Trong thời đại Kỹ thuật số hiện nay, vấn đề vi phạm bản quyền và sao chép bất hợp pháp dữ liệu là phổ biến. Hải đồ hàng hải điện tử (ENC) cũng gặp phải những vấn đề này. Việc phân phối không chính thức các thông tin hàng hải làm ảnh hưởng đến sự an toàn hàng hải và nền kinh tế. Kết quả là, người xuất bản thông tin hàng hải chính thức đã tìm cách bảo mật dữ liệu của họ và cung cấp thông tin chính xác cho các nhà hàng hải thông qua một lược đồ bảo vệ.

Tháng 9 năm 2000, các quốc gia thành viên của Tổ chức thủy đạc quốc tế (IHO)được thăm dò về tầm nhìn của họ trong việc phát triển một Lược đồ bảo mật dữ liệu do IHO đề nghị (RSS-Recommended Security Scheme) (xemThông tư 38/2000 của Cục thủy đạc quốc tế). Các phản hồi cho thấy rằng các quốc gia thành viên mong muốn dữ liệu ENC của mình được mã hóa và chấp nhận đề nghị của IHO về RSS (xem Thông tư 15/2001 của Cục thủy đạc quốc tế). Đa số các quốc gia thành viên hưởng ứng, chấp nhận Lược đồ bảo mật Primar (Primar Security Scheme) như IHO RSS. Như vậy tại thời điểm này theo thông lệ tiêu chuẩn bảo mật dữ liệu ENC và đa số các nhà sản xuất ECDIS đã triển khai các tiện ích giải mã cần thiết trong hệ thống của họ.

Ủy ban về tiêu chuẩn hệ thống thông tin thủy đạc(CHRIS – Committee on Hydrographic Requirements for Information System), nay gọi là Ủy ban dịch vụ và tiêu chuẩn thủy đạc (HSSC – Hydrographic Services and Standards Committee), tại hội nghị lần thứ 13 (Athens, Greese, tháng 9 năm 2001)đã kiểm tra lại các vấn đề của RSS1và đồng ý lập một nhóm nghiên cứu chịu trách nhiệm phát triển Lược đồ bảo mật RSS phù hợp với tiêu chuẩn của Cục thủy đạc quốc tế (IHB).

Tháng 1 năm 2002, Nhóm quản trị lược đồ bảo vệ dữ liệu(DPSWG- Data Propection Scheme Working Group) đã báo cáo tới IHB về kế hoạch phát triển một lược đồ bảo vệ dữ liệu IHO RSS phiên bản 1. Báo cáo này đã được Ủy ban về tiêu chuẩn hệ thống thông tin thủy đạc (CHRIS) thông qua vào tháng 2 năm 2002.

Tại hội nghị lần 14 của IHO (Thượng hải, Trung Quốc, tháng 8 năm 2002), Ủy ban về tiêu chuẩn hệ thống thông tin thủy đạc (CHRIS) đã báo cáo về lược đồ bảo vệ dữ liệu IHO RSS 1 và vai trò Quản trị Lược đồ bảo vệ được chuyển giao cho IHO. Báo cáo này được các nước thành viên thông qua và được đặt tên là S-63 vào tháng 10 năm 2003.

Tại Hội nghị lần thứ 18 (Cairns, Australia, tháng 9 năm 2006), Ủy ban về tiêu chuẩn hệ thống thông tin thủy đạc (CHRIS) đã giao cho Nhóm quản trị lược đồ bảo vệ dữ liệu (DPSWG) xuất bản Tiêu chuẩn S63 với quy định như sau:

Không giới thiệu về các đối tượng mới; hạn chế tối đa các thay đổi.

Nguyên tắc chỉ đạo mà Tiêu chuẩn S-63 công bố sẽ được đưa vào trong tiêu chuẩn.

Tổ chức lại Tiêu chuẩn S-63 thành các nhóm theo quy định của Cục thủy đạc quốc tế (IHB): Lược đồ quản trị, nhà phân phối (data server)và nhà sản xuất thiết bị gốc (OEM).

Kèm theo miêu tả chính xác các hiệu chỉnh bổ sung theo tiêu chuẩn IHO.

Do đó, tại hội nghị lần thứ 19 (Rotterdam, Hà Lan, tháng 11 năm 2007) Ủy ban về tiêu chuẩn hệ thống thông tin thủy đạc (CHRIS) đã thông qua Phiên bản 1.1 của S-63 của Nhóm quản trị lược đồ bảo vệ dữ liệu (DPSWG). Phiên bản này được các nước thành viên thông qua và có hiệu lực vào tháng 3 năm 2008. Phiên bản 1.1 –S63 bao gồm tài liệu hỗ trợ, dữ liệu kiểm tra và phương thức cung cấp ENCs sử dụng "hỗ trợ thông tin lớn" ("Large Media Support").

Tháng 4 năm 2012, phiên bản 1.1có sự thay đổi nhỏ, trong đó xóa bỏ các nhược điểm hệ số thập lục phân của M_ID để mở rộng giá trị M_ID nhằmđáp ứng cấu trúclược đồ. Theo đó, phiên bản 1.1.1 của S-63 ra đời thay thế phiên bản 1.1 trước đó.Sự thay đổivà phát triển tiêu chuẩn này sẽ được DPSWG tiếp tục dướisự hướng dẫn của HSSC.

Mục lục

Bảng chú giải

Bảng chú giải cho các thuật ngữ dùng trong Lược đồ bảo vệ dữ liệu S-63

Blowfish	Thuật toán mã hóa đượcsử dụng trongLược đồ bảo vệ dữ liệu.
Cell Key	Khóa được sử dụng để mã hóaENC và được yêu cầu để giải mã ENC đã mã hóa.
Data Client	Thuật ngữ dùng để miêu tả người dùng cuối cùng nhận thông tin ENC đã mã hóa.Data Client sẽ sử dụng ứng dụng phần mềm (ví dụ ECDIS) để thực hiện những phân tích trong lược đồ. Đặc biệt là người sử dụng ECDIS.
Data Server	Thuật ngữ dùng để miêu tả tổ chức mã hóa ENC hoặc phát hành Cell Permittới người sử dụng.
M_ID	Mã định danh duy nhất được ấn định bởi Nhà quản trị Lược đồ (SA)cho mỗi nhà sản xuất ECDIS. Data Servers sử dụng mã này để xác nhận M_KEY khi giải mã Userpermit.
M_KEY	Khóa nhận dạng duy nhất của nhà sản xuất ECDIS được cung cấp bởi Nhà quản trị Lược đồ (SA) tới OEM (nhà sản xuất thiết bị). OEM sử dụng nó để mã hóa HW_ID khi tạo ra Userpermit.
HW_ID	Mã định danh duy nhất được OEM gán cho hệ thống của họ. HW_ID được mã hóa bằng cách sử dụng M_KEY duy nhất của OEM và được cung cấp tới Data Client như một Userpermit. Phương thức này cho phép Data Client có thể mua giấy phép sử dụng để giải mã các dữ liệu ENC đã mã hóa.
SA	Nhà quản trị Lược đồđại diện cho IHO.
SHA-1	Thuật giảiBăm An Toàn [3].
SSK	Khóa tự ký (Tập tin chứng chỉ tự ký) được tạo ra bởi Data Server bằng cách dùng khóa riêng Private Key kí vào khóa chung Public Key.
User Permit	Giấy phép người dùng (User Permit) là dạng mã hóa của giá trị HW_ID,mỗi hệ thống ECDIS có duy nhất một mã User Permit để nhận biết.

Thuật ngữ liên quan đến hải đồ

ECDIS	Hệ thống thông tin và hiển thị hải đồ điện tử theo quy định của IMO.
ENC	Hải đồ hàng hải điện tử theo định nghĩa trongChi tiết kỹ thuật sản phẩm ENC (ENC Product Specification) [1].
S-57	Tiêu chuẩn chuyển đổi cho ENC định nghĩa bởi IHO.
SENC	Hệ thống ENC (đây là định dạng bên trong để OEM chuyển đổi khi nhập dữ liệu).

Các tổ chức

ECC	Trung tâm hải đồ điện tử AS (Electronic Chart Centre AS) (www.ecc.as).
HO	Cơ quan thủy đạc (ví dụ: Data Server).
IHB	Cục Thủy đạc Quốc tế.
IHO	Tổ chức Thủy đạc Quốc tế.
IMO	Tổ chức Hàng hải Quốc tế.
RENC	Trung tâm phối hợp vùng ENC, hợp nhất các ENC từ nhiều cơ quan thủy đạc thành một dịch vụ duy nhất (ví dụ: Data Server).
UKHO	Cơ quan thủy đạc Vương quốc Anh (www.ukho.gov.uk).

Thuật ngữ tin học.

CRC	Kiểm tra tình trạng dư thừa theo chu kỳ (Cyclic Redundancy Check)
Dongle	Được xem như thiết bị khóa cứng, nó là thiết bị phần cứng được cung cấp bởi OEM với mã định danh duy nhất của hệ thống (HW_ID) được lưu trữ an toàn bên trong.
XOR	Độc quyền OR (Exclusive OR).

1 GIỚI THIỆU CHUNG

Ấn phẩm "Lược đồ Bảo vệ Dữ liệu IHO S-63", gọi tắt là "Lược đồ", miêu tả tiêu chuẩn được đưa ra để bảo vệ thông tin ENC. Nó định nghĩa cấu trúc bảo vệ và quy trình hoạt động phải được tuân thủ để đảm bảo rằng Lược đồ bảo vệ dữ liệu được vận hành đúng và cung cấp các chi tiết kỹ thuật cho phép các thành phần tham gia xây dựng hệ thống tuân theo S-63 và phân phối dữ liệu an toàn và theo cách có thể thực hiện được về mặt thương mại.

Lược đồ bảo vệ dữ liệu được xây dựng bởi Nhóm quản trị Lược đồ bảo vệ dữ liệu (DPSWG) của IHO. Tiêu chuẩn S-63 dựa trên lược đồ bảo vệđược Công tyPrimar và Primar-Stavanger phát triển và tiến hành như một phần của dịch vụ bảo vệ dữ liệu ENC của cơ quan này. Trung tâm Hải đồ điện tử AS và Cơ quan Thủy đạc Vương quốc Anh là các tổ chức tham gia đầu tiên.

Tháng 12 năm 2002 (IHO CL 66, 2002), bộ tiêu chuẩn nàyđược chấp nhận bởi các nước thành viên IHO và trở thành tiêu chuẩn chính thức của IHO. Bộ tiêu chuẩn nàyquy định vai trò và trách nhiệm của các cơ quan thủy đạc quốc gia trong việc bảo vệ dữ liệu ENC và phân phối tới người sử dụng hệ thống ECS/ECDIS.

1.1 Mô tả khái quát

Tài liệu này quy định phương pháp bảo mật thông tin ENC và duy trì tính toàn vẹn của dịch vụ ENC với nhiều dịch vụ dữ liệu đáp ứng nguồn khách hàng lớn. Mục đích của việc bảo vệ dữ liệu gồm 3 phần:

1. Bảo vệ sự vi phạm bản quyền: Ngăn ngừa việc sử dụng trái phép dữ liệu bằng cách mã hóa thông tin ENC.
2. Truy cập có chọn lọc: Hạn chế truy cập thông tin ENC, chỉ các Cell mà khách hàng có giấy phép mới được truy cập.
3. Chứng thực dữ liệu (Authentication): Cung cấp sự đảm bảo dữ liệu ENC tới từ các nguồn đã được thông qua.

Bảo vệ sự vi phạm bản quyền và hạn chế truy cập có chọn lọc được thực hiện bằng cách mã hóa thông tin ENC và cung cấp các giấy phép để giải mã chúng. Nhà phân phối dữ liệu(Data Server) sẽ mã hóa dữ liệu ENC được cung cấp bởi nhà sản xuất trước khi cung cấp nó cho khách hàng (Data Client). Các ENC đã mã hóa sau đó được giải mã bằng ECS/ECDIS trước khi được định dạng lại và nhập vào hệ thống SENC. Quá trình chứng thực dữ liệu (authentication) được quy định bằng phương pháp Chữ ký số vào trong dữ liệu.

Lược đồ không quy định cách thông tin ENC hoặc SENC được bảo vệ bên trong một ứng dụng người dùng cuối cùng.Đây là trách nhiệm của các OEM.

Lược đồ cho phép phân phối đa số các ENC đã mã hóa trên đĩa cứng (ví dụ: CD-ROM, DVD) và có thể được truy cập, được sử dụng bởi tất cả khách hàng có giấy phép hợp lý chứa trong một tập giấy phép (permit). Lựa chọn truy cập tới các Cell riêng lẻ được hỗ trợ bằng cách cung cấp cho người dùng một giấy đăng ký gồm một tập đăng kýgiấy phép chứa Khóa mã hóa Cell.Giấy đăng ký này được tạo ra bằng cách sử dụng một mã định danh phần cứng (HW_ID) duy nhấtcủa hệ thống và từ yêu cầu của mỗi khách hàng.Vì vậy, giấy đăng ký không được chuyển đổi giữa các khách hàng riêng rẽ.

Lược đồ sử dụng thuật toán nén để giảm kích cỡ tập dữ liệu.Dữ liệu ENC không được mã hóa thường có sự lặp đi lặp lại thông tin, ví dụ như thông tin tọa độ. Vì vậy, việc nén dữ liệu luôn được áp dụng trước khi thông tin ENC được mã hóa và giải nén sau khi giải mã trên hệ thống của khách hàng (thông thường là ECS/ECDIS).

1.2 Thành phần tham gia Lược đồ

Các đối tượng sử dụng Lược đồ, bao gồm:

- Nhà quản trị Lược đồ (Scheme Administrator-SA), là duy nhất.
- Nhà phân phối dữ liệu (Data Server-DS), có thể có nhiều.
- Khách hàng (Data Client-DC), có thể có nhiều.
- Công ty sản xuất thiết bị phần cứng (OEM), có thể có nhiều.

Thông tin chi tiết về các thuật ngữ này được giải thích phía dưới.

1.2.1 Nhà quản trị Lược đồ (Scheme Administrator)

Nhà quản trị lược đồ (SA) là cơ quan duy nhất, chịu trách nhiệm về duy trì và phối hợp lược đồ.Vai trò của SA được điều hành bởi IHB, giống như ban thư ký của IHO, thay mặt cho các nước thành viên của IHO.

SA chịu trách nhiệm về việc kiểm soát số hội viên của lược đồ và đảm bảo tất cả những người tham gia vận hành theo các thủ tục đã được xác định. SA duy trì chứng chỉ số ở mức cao nhất để vận hành Lược đồ Bảo mật dữ liệu hải đồ điện tử(S-63) và là cơ quan duy nhất có thể chứng nhận đặc tính của những người tham gia vào Lược đồ.

SA cũng chịu trách nhiệm về tất cả các tài liệu liên quan đến Lược đồ Bảo mật dữ liệu hải đồ điện tử(S-63).

1.2.2 Nhà phân phối dữ liệu ENC (Data Servers)

Data Servers chịu trách nhiệm mã hóa và ký vào dữ liệu ENC tuân theo các thủ tục và phương pháp được quy định trong lược đồ. Data Servers phát hành giấy đăng ký ENC (giấy phép) cho các Data Client, với giấy phép người dùng hợp lệ, có thể giải mã dữ liệu ENC.

Data Servers sử dụng thông tin M_KEY và HW_ID, được cung cấp bởi SA để phát hành các Cell Key ENC đãmã hóa cho từng cài đặt cụ thể. Mặc dù Cell Key sử dụng để mã hóa cho từng Cell là giống nhau, chúng sẽ được mã hóa bằng cách sử dụng HW_ID duy nhất và vì vậy không thể chuyển giao giữa các hệ thống ECDIS khác nhau từ cùng một nhà sản xuất.

Các Cơ quan Thủy đạc,các đại lý phân phối và các tổ chức RENC đều được xem là Data Server.

1.2.3 Khách hàng (Data Clients)

Data Clients là người cuối cùng sử dụngcác thông tin ENC và nhận thông tin được bảo vệ từ Data Server. Các ứng dụng phần mềm của Data Clients (hệ thống OEM) chịu trách nhiệm xác nhậnchữ ký số ENC và giải mã thông tin ENC tuân theo các thủ tục được định rõ trong lược đồ.

Những người đi biển với hệ thống ECDIS/ECS được xem là Data Client.

Lược đồ không đề cập đến các đại lý hoặc các nhà phân phối cung cấp dữ liệu phục vụ cho khách hàng của họ. Các thỏa thuận và cấu trúc đạt được này nằm ngoài phạm vi của tài liệu. Tài liệu này chỉ chứa các chi tiết kỹ thuật để tạo ra các hệ thống và dịch vụ dữ liệu tuân theo S-63.

1.2.4 Nhà sản xuất thiết bị phần cứng - (OEM - Original Equipment Manufacturers)

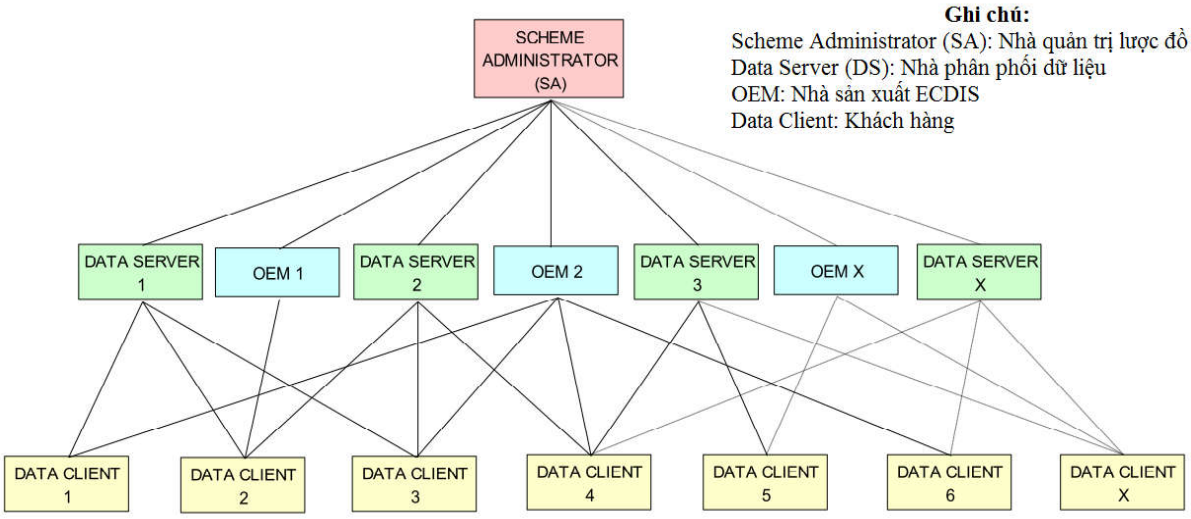
Các OEM đăng ký với Lược đồ Bảo mật dữ liệu hải đồ điện tử(IHO S-63 DPS) phải xây dựng một ứng dụng phần mềm theo các chi tiết kỹ thuật đặt ra trong tài liệu này và tự kiểm tra, xác nhận nó theo các điều khoản được yêu cầu bởi SA. Tiêu chuẩn S-63 chứa các dữ liệu thử nghiệm cho việckiểm tra và xác nhận các ứng dụng OEM.SA sẽ cung cấp đầy đủ cácthành phần OEM với các mã định danh và khóa nhận dạng (M_ID và M_KEY) duy nhất của riêng họ.

Các nhà sản xuất cần phải cung cấp cơ chế an toàn bên trong hệ thống phần mềm của họ để nhận biết duy nhất từng sự cài đặt người dùng cuối cùng. Lược đồ yêu cầu mỗi sự cài đặt có một mã định danh phần cứng riêng (HW_ID).

Các ứng dụng phần mềm có khả năng giải mã các Cell Key bằng cách sử dụng HW_ID được lưu trữ trong các thiết bị khóa cứng hoặc khóa mềm được gán vào hoặc lập trình sẵn bên trong ứng dụng để giải mã và giải nén dữ liệu ENC. Giá trị CRC chứa trong ENC[1] sau đó có thể được xác minhđể chứng minh tính toàn vẹn làm nền tảng cho dữ liệu S-57.

1.2.5 Mối quan hệ giữa cácthành phần tham gia lược đồ S-63 (S-63 Participant Relationships)

Nhà quản trị Lược đồ (SA) là tổ chức duy nhất có quyền nhận diện các thành phần tham giavào Lược đồ. Tất cả các Nhà phân phối và Hệ thống các nhà sản xuất (OEMs) phải xin phép SA để trở thành thành viên trong lược đồ và được SA cung cấp thông tin độc quyền duy nhất tới họ. Data Clients là các khách hàng của Data Servers và OEMs nơi màData Server cung cấp các dịch vụ



Mối quan hệ trong Lược đồ bảo vệ dữ liệu S-63

dữ liệu và OEMs cung cấp các thiết bị để giải mã và hiển thị các dịch vụ này.

1.3 Tài liệu tham khảo

[1] S-57 phiên bản 3.1: Tiêu chuẩn chuyển đổi IHO dành cho dữ liệu thủy văn số. (www.iho.int).

[2] Tiêu chuẩn chữ ký số (DDS-Digital Signature Standard) FIPS Pub 186(www.itl.nist.gov/div897/pubs/fip186.htm).

[3] Tiêu chuẩn Băm an toàn (SHA), FIPS Pub 180-1 (www.itl.nist.gov/div897/pubs/fip180-1.htm).
[4] Công nghệ thông tin –Mối quan hệ các hệ thống mở - Thư mục: Chứng thực Framewwork. Phiên bản X.509 – Liên đoàn Viễn thông Quốc tế.
[6] Chi tiết kỹ thuật định dạng tập tin ZIP, PKWare Inc.
[7] Chế độ DES của hệ điều hành, FIPS Pub 81 (www.itl.nist.gov/fipspubs/fip81.htm).
[8] RFC 1423: Tăng cường bảo mật cho thư điện tử mail: phần III: Giải thuật, chế độ và nhận biết (ftp://ftp.isi.edu/in-notes/rfc1423.txt).
[9] Thuật toán mã hóa Blowfish, B. Schneier, Fast Software Encryption, Cambridge Security Workshop.
Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204. (www.counterpane.com).
[10] Thuật toán Checksum CRC32. Công nghệ thông tin – viễn thông và thông tin chuyển đổi giữa các hệ thống - High-level data link control (HDLC) procedures. ISO/IEC 13239:2002.

1.4 Khả năng tương thích với các phiên bản trước

Phiên bản S-63 này sử dụng cùng thuật toán, cùng định dạng tập tin và cùng nội dung như Lược đồ bảo vệđược điều hành bởi Primar, Primar-Stavanger và lược đồ S-63phiên bản 1.0.Phiên bản này của Tiêu chuẩn S-63 được sửa đổi để cung cấp tốt hơn các định nghĩa và giải thích về hoạt động của Lược đồ Bảo vệ.

Mộtbộ dữ liệu dùng thử đã được xây dựng và được sử dụng bởi các OEM để kiểm tra và xác nhận việc triển khai Lược đồ Bảo mật dữ liệu hải đồ điện tử(S-63) trong quá trình tự cấp giấy chứng nhận.

Phiên bản 1.1 của Tiêu chuẩn này được sản xuất dựa trên kinh nghiệm có được của các Data Servers và các nhà sản xuất ECS/ECDIS trong quá trình vận hành Lược đồ phiên bản 1.0. Phiên bản này định nghĩa rõ hơn các tiêu chuẩn bằng cách loại bỏ sự trùng lặp và không rõ ràng. Nó cũng bổ sung các cơ chế cho phép nhà sản xuất tạo ra hệ thống trực quan hơn cho người sử dụng ECS/ECDIS. Danh sách dưới đây đề cập đến các điều chỉnh trong tiêu chuẩn này:

1. Loại bỏ sự trùng lặp không cần thiết.
2. Chi tiết kỹ thuật nào và trong những điều kiện nào thì tập tin phải được sử dụng.
3. Loại bỏ các giấy phép phụ thuộc vào phiên bản Cell.
4. Bổ sung thông tin cho phép Data Client quản lý dữ liệu ENC hiệu quả và có ích hơn.
5. Xác định một chiến lược tải cho phép tải hiệu quả hơn các ENC đã mã hóa.

Đây là trách nhiệm của Data Server để cung cấp các dịch vụ có thể tương thích ngược.

1.5 Cấu trúc tài liệu

Tài liệu này chia làm bốn phần chính.Phần thứ nhất mô tả chi tiết các thành phần nền tảng của Lược đồ và miêu tả mục đích, cấu trúc của lược

đồ.Phần thứ 2 xác định làm cách nào để tất cả các thành phần kết hợp với nhau trong một Bộ sản phẩm trao đổi ENC S-63 (ENC Exchange Set).Phần thứ 3 chỉ ra vai trò và trách nhiệm của từng người dùng tham gia vào Lược đồ.Phần cuối cùng miêu tả định nghĩa các thông báo lỗi và cảnh báolỗi khác nhau cần được hiển thị trên hệ thống của khách hàng.

Các phần chính của tài liệu:

1. Các thành phần của Lược đồ
   Phần 2: Nén dữ liệu
   Phần 3: Mã hóa dữ liệu
   Phần 4: Cấp giấy phép dữ liệu
   Phần 5: Xác nhận dữ liệu
   Phần 6: Quản lý dữ liệu
1. Cấu trúc và định dạng Bộ sản phẩm trao đổi (Exchange Set)
   Phần 7: Cấu trúc Tập tin và Thư mục
2. Quy trình tham gia S-63
   Phần 8: Tiến trình của Nhà quản trị Lược đồ
   Phần 9: Tiến trình của Data Server
   Phần 10: Tiến trình của OEM và Data Clients
3. Các cảnh báo và thông báo lỗi trong S-63
   Phần 11: Mã lỗi và giải nghĩa

Phần bổ sung:

- Phụ Chương A S-63: Thủ tục yêu cầu giấy chứng nhận Data Server
- Phụ chương B S-63: Thủ tục yêu cầu thông tin nhà sản xuất

Các phụ lục:

- Phụ lục 1: Chứa định nghĩa về dữ liệu dùng thử sẵn có được sử dụng để phát triển toàn diện, tuân theo tất cả các khía cạnh của Lược đồ Bảo vệ Dữ liệu.
- Phục lục 2: Định nghĩa thế nào là Bộ sản phẩm trao đổi ENC đã mã hóa được cung cấp bởi Data Server sẽ được lưu trữ bằng cách sử dụng thiết bị lưu trữ như đĩa DVD hoặc USB.

1.6 Bảo trì

Các thay đổi trong tiêu chuẩn này phải phù hợp với *"Các nguyên tắc và thủ tục làm thay đổi các tiêu chuẩn và chi tiết kỹ thuật IHO*" được phê duyệt tại cuộc họp CHRIS lần thứ 18 (Cairns, Úc, tháng 9 năm 2006).

1.7 Hỗ trợ

Hỗ trợ trong việc sử dụng và thực hiện tiêu chuẩn này được cung cấp cho người sử dụng bởi các thành viên của IHO DPSWG, qua cuộc thảo luận về Lược đồ bảo vệ trên các diễn đàn ECDIS (www.openecdis.org). Ngoài ra, tập danh mục các câu hỏi thường gặp (FAQ) được duy trì bởi IHB trên phần ECDIS của trang web IHO (www.iho.int)

2 NÉN DỮ LIỆU

2.1 Tổng quan

Một tập tin ENC sẽ có cấu trúc của nó, chứa các mẫu thông tin lặp đi lặp lại. Ví dụ: việc đánh số liên tiếp các mã định danh đối tượng tính năng (FOID) hoặc các thay đổi nhỏ về thông tin tọa độ bên trong một tập tin ENC. Do đó, dữ liệu ENC cần được nén để giảm kích cỡ từ khoảng 30% đến 60%, giảm đáng kể chi phí chuyển giao dữ liệu ENC đến người dùng. Chỉ các tập tin ENC nền và ENC cập nhật là được nén. Các tập tin ENC luôn được nén trước khi chúng được mã hóa như hiệu lực của thuật toán nén dựa trên sự hiện diện của nội dung cấu trúc dữ liệu.

2.2 Thuật toán nén

Lược đồ bảo vệ sử dụng thuật toán ZIP [6][1] để nén và giải nén dữ liệu ENC. Nó tương tự với thuật toán được sử dụng trong nhiều ứng dụng thương mại như WinZip, PKZIP,…Data Server và OEM nhận biết được các lỗi trong quá khứ đã xảy ra khi Data Server nén dữ liệu và nó được giải thích bởi việc triển khai thuật toán ZIPphổ biến như dữ liệu “text”.

Nếu dữ liệu được giải nén với các tham số không chính xác, nó có thể làm hỏng tập tin ENC dẫn đến thất bại trong kiểm tra tính toàn vẹn.Data Server và OEM nên thực hiện cẩn thận việc nén/giải nén trong hệ thống của họ.

2.3 Nén tập tin

Các Lược đồ bảo vệ chỉ nén các tập tin ENC nền (base cell) và cập nhật (update cell). Không có tập tin nào khác bên trong Bộ sản phẩm trao đổi S-57 (S-57 Exchange Set) được nén.

[1] http://en.wikipedia.org/wiki/ZIP_%28file_format%29

3 MÃ HÓA DỮ LIỆU

3.1 Dữ liệu nào được mã hóa?

Chỉ có một thuật toán mã hóa được sử dụng trong Lược đồ. Chỉ các dữ liệu trong tập tin Cell ENC Base và Update của Bộ sản phẩm trao đổi S-57 được mã hóa, tức là các tập tin text và hình ảnh không được mã hóa.

Lược đồ mã hóa toàn bộ nội dung của tập tin dữ liệu ENC Base và Update. Các thông tin khác trong Lược đồ được mã hóa bao gồm mã HW_IDcủa hệ thống OEM được mã hóa và cung cấp tới Data Client dưới dạng User Permit.

Data Server sử dụng Cell Key để mã hóa tập tin dữ liệu ENC và cung cấp cho Data Clientdưới dạng Cell Permit. Thông tin về thuật toán mã hóa có sẵn trong phần 3.2.3.

3.2 Mã hóa dữ liệu như thế nào?

Mỗi một tập tin Cell ENC được mã hóa bằng cách sử dụng giá trị Cell Key duy nhất.Cùng một Cell Key được sử dụng để mã hoá tất cả các bản cập nhật được phát hành cho các Cell. Tuy nhiên, Lược đồ chỉ cho phép các Cell Key được gia hạn và được thay đổi theo quyết định của Data Server. Các Cell Key được chuyển đến cho Data Client dưới dạng Cell Permits.

3.2.1 Mã hóa thông tin ENC

Thông tin ENC (các Cell base và update) được mã hóa bằng cách sử dụng một khóa 40 bit.

3.2.2 Mã hóa thông tin Lược đồ bảo vệ khác

Nội dung Userpermit và Cell Permit được mã hóa bằng cách sử dụng một khóa 48 bit.

3.2.3 Thuật toán mã hóa - Blowfish

Lược đồ mã hóa tất cả các thông tin được đề cập trong phần 3.1 bằng cách sử dụng thuật toán Blowfish [9]. Thuật toán không có bằng sáng chế và có sẵn trong phạm vi công khai (www.counterpane.com). Blowfish là thuật toán mã hóa khối vận hànhvớisố lượng 64 bit (8 byte). Nó đòi hỏi các nguồn dữ liệu phải được đệm thêm nếu chúng không phải là bội số của 8 bytes.Lược đồ Bảo vệ sử dụng thuật toán đệm thêm"DES in CBC Mode" để xác định trong bất cứ khi nào nguồn dữ liệu cần phải đệm thêm [8].Điều này phù hợp với chế độ ECB (Electronic Code Book – Mã số sách điện tử) của DES [7].

4. CẤP GIẤY PHÉP DỮ LIỆU

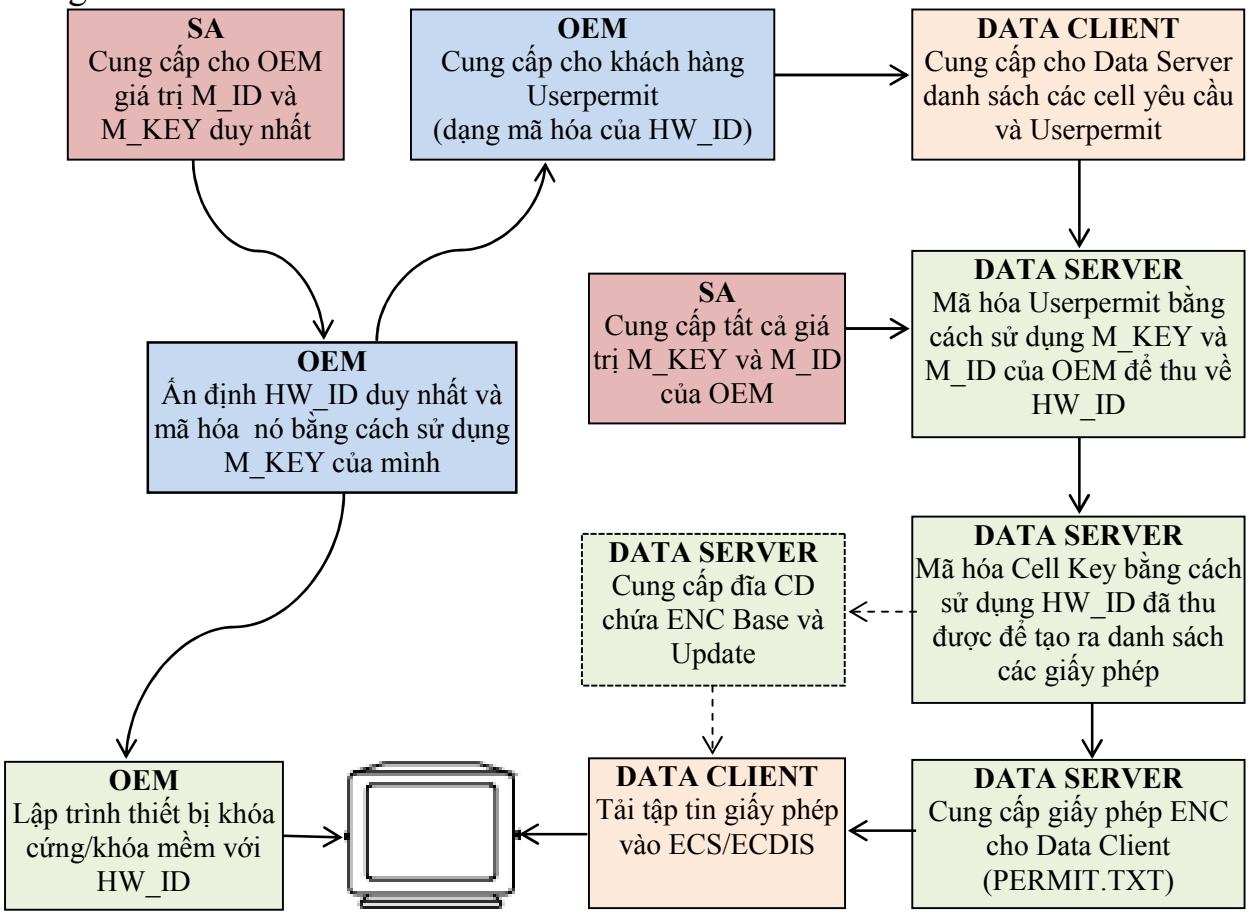
4.1 Giới thiệu

Data Client không mua dữ liệu ENC nhưng được cấp giấy phép để sử dụng nó.Cấp giấy phép là phương pháp mà Data Server sử dụng nhằm cung cấp cho Data Client truy cập chọn lọc để cập nhật các cell ENC trong một khoảng thời gian nhất định.

Để vận hành Lược đồ hiệu quả cần phải có một phương pháp mà hệ thống của Data client có thể giải mã các Cell ENC đã mã hóa. Để giải mã dữ liệu, hệ thống Data client cần phải có quyền truy cập vào Cell Key đã được sử dụng để mã hóa các Cell ENC. Các khóa này được cung cấp cho Data Client, được mã hóatrong một tập tin giấy phép chứa một bộ Cell Permit. Đó là các Cell Permit chứa các khóa mã hóa.

Để tạo tập Cell Permit độc quyền thì các Cell Key phải được mã hóa duy nhất cho hệ thống Data Clients.OEMs gán một mã định danh duy nhất (HW_ID) cho mỗi hệ thống của họ và cung cấp một bản sao đã mã hóa này dưới dạng UserPermit cho mỗi Data Client.HW_ID được lưu trữ trong UserPermit đã mã hóa.

Các OEM mã hóa HW_ID với khóa nhà sản xuất riêng của mình (M_Key) sao cho một HW_ID không bị lặp lại bởi nhà sản xuất khác. Data Server có thể truy cập tới M_Key của OEM và do đó có thể giải mã HW_ID lưu trữ trong Userpermit. Data Server mã hóa các Cell Key của chúng với mã HW_ID của nhà sản xuất khi tạo ra một tập các Cell Permit.Điều này giúp cho các Cell Permit là duy nhất khi cung cấp cho Data Client và vì vậy không thể chuyển giao giữa các hệ thống Data Client.



4.2 Giấy phép người dùng (User Permit)

Userpermit được tạo bởi OEM và được cung cấp cho Data Clients như một phần hệ thống của họ sao cho chúng có thể được quyền truy cập cần thiết tới các ENC đã mã hóa từ Data Server.Phần sau đây xác định thành phần và định dạng của Userpermit.

Tất cả Data Client với hệ thống có khả năng sử dụng dữ liệuđược bảo vệ bởi Lược đồ S-63, phải có mã nhận dạng phần cứng (HW_ID)duy nhất gắn vào trong hệ thống người dùng cuối cùng.Như thế, một HW_ID thường được triển khai như một thiết bị chống sao chép lậu (dongle) hoặc bằng phương pháp khác để đảm bảo chỉ nhận biết duy nhất cho mỗi sự cài đặt.

Data Clientkhông biếtHW_ID, nhưng OEM sẽ cung cấp một Userpermit là dạng mã hóa của HW_ID và là duy nhấtcho hệ thống của Data Client.User Permit được tạo ra bằng cách lấy HW_ID được ấn định và mã hóa nó với khóa nhà sản xuất (M_KEY).Thuật toán CRC32 được sử dụng để mã hóa HW_ID và kết quả được gán thêm vào nó. Cuối cùng, nhà sản xuất gắn mã M_ID mà họ được ấn định vào cuối chuỗi kết quả.Các giá trị M_KEY và M_ID được cung cấp bởi SA và là duy nhất cho mỗi nhà sản xuất cung cấp hệ thống phù hợp vớiS-63.

Data Client truy cập được vào ENCs đã mã hóa theo S-63 bằng cách cung cấp Userpermit này cho Data Server, người mà sau đó có thể phát hành các Cell Permit riêng biệt cho ENCs đãmã hóa. Vì Userpermit chứa mã nhà sản xuất (M_ID) duy nhất này có thể được sử dụng bởi Data Servers để nhận biết M_KEY sử dụng để giải mã nó.M_ID là 4 ký tự cuối của User Permit.Danh sách giá trị M_ID và M_KEY của nhà sản xuất được phát hành và cập nhật bởi SA tới tất cả Data Server tham gia lược đồ.Danh sách này sẽ được cập nhật định kỳ khi các OME mới tham gia vào lược đồ.

4.2.1 Định nghĩa UserPermit

Userpermit gồm 28 ký tự và sẽ được viết dưới dạng ASCII với định dạng bắt buộc và chiều dài như sau:

Dạng mã hóa của HW_ID	Checksum (CRC)	Mã nhà sản xuất (M_ID)
16 ký tự hex	8 ký tự hex	4 ký tự hex

Hex: số thập lục phân.

Tất cả ký tự chữ cái phải được viết hoa.

Ví dụ: Cấu trúc User Permit:

73871727080876A07E450C043031

Dạng mã hóa của HW_ID — CRC — M_ID

4.2.2 Định dạng HW_ID

HW_ID là một số hệ thập lục phân 5 ký tự được xác định bởi nhà sản xuất OEM. Như vậy, HW_IDcó thể được thi hành như một thiết bị chống sao chép lậu (Dongle - khóa cứng) hoặc bằng các phương pháp khác để bảo đảm nhận biết duy nhất cho mỗi hệ thống cài đặt[2]. HW_ID phải được lưu trữ trong hệ

[2]Nhà sản xuất, với sự đồng ý của Data Server, có thể sử dụng HW_ID giống nhau cho nhiều sự cài đặt.

thống hết sức bảo mật.

Nhà sản xuất OEM phải gán mã HW_ID duy nhất cho mỗi hệ thống cài đặt. Nó được khuyến cáo rằng: HW_ID không nên liên tục.

HW_ID sẽ được lưu trữ ở dạng mã hóa của Userpermit. Nó được mã hóa bằng cách sử dụng thuật toán Blowfish với M_KEY như một khóa để đưa ra một sốthập lục phân 16ký tự (8 byte). HW_ID được mã hóa sau đó được biểu diễn dạng ASCII của nó trong Userpermit gồm 16 ký tự.

Ví dụ về HW_ID là: **A79AB**

Ví dụ về dạng mã hóa HW_ID là: **73871727080876A0.**

4.2.3 Định dạng Check Sum (CRC)

Check Sum là một số thập lục phân 8 ký tự, được tạo ra bằng cách lấy HW_ID đã mã hóa và chuyển đổi thành một chuỗi thập lục phân 16 ký tự. Sau đó nó được chia ra bằng cách sử dụng thuật toán CRC32[10] và 4 byte được chuyển đổi thành một chuỗi thập lục phân 8 ký tự.

Check Sum không được mã hóa và dùng để kiểm tra tính toàn vẹn của Userpermit.

Check Sum trong ví dụ trên là: **7E450C04.**

4.2.4 Định dạng M_ID

M_ID là một mã gồm 2 ký tự chữ-sốtrình bày dạng ASCII được cung cấp bởi SA.SA sẽ cung cấpcho cácnhà sản xuất được cấp phép một tổ hợp M_KEY và M_ID của riêng mình.Các nhà sản xuất phải bảo vệ thông tin này.

SA sẽ cung cấp tới tất cả Data Servers được cấp phép một danh sách đầy đủ các mã nhà sản xuất cũng như khi một nhà sản xuất mới đăng ký vào Lược đồ. Thông tin này được sử dụng bởi Data Server để xác định các khóa (M_KEY) sử dụng để giải mã HW_ID trong Userpermit khi tạo ra Cell Permits cho Data Client.

M_ID trong ví dụ trên là 01 hoặc 3031 (ASCII[3]).

4.2.5 Định dạng M_KEY

M_KEY là một số thập lục phân 5 ký tự, được cung cấp bởi SA. Các OEM sử dụng M_KEYđể mã hóa HW_ID khi tạo ra Userpermit.OEM phải lưu trữ M_KEY hết sức bảo mật.M_KEY được sử dụng bởi Data Server để giải mã HW_ID được ấn định.

Ví dụ về M_KEY là **123AB** hoặc **3132334142** (ASCII).

4.3 Cell Permit

Để giải mã một Cell ENC thì Data Client phải có quyền truy cập vào các khóa mã hóa (xem phần 3.2) được sử dụng để mã hóa Cell ENC này.Vì khóa mã hóa chỉ có Data Server biết, cho nêncần có biện pháp cung cấp thông tin này tới Data Client một cách bảo mật. Thông tin này được Data Server (ví dụ RENC hoặc VAR) cung cấp cho Data Client ở dạng mã hóa, được biết đến là Cell Permit. Một tập tin duy nhất được quy định để cung cấp Cell Permit và được đặt tên là PERMIT.TXT (xem phần 4.3.1). Tập tin này có thể chứa nhiều Cell Permit dựa trên số lượng ENC được yêu cầu bởi Data Client.

[3] Lưu ý: Các mã hex có thể không quen thuộc với một số đọc giả. Vì lý do lịch sử, nó vẫn được bảo tồn trong phiên bản này như các tiêu chuẩn. “1 2 3 4 5” được dịch thành “31 32 33 34 35” bởi vì ASCII Base 16, miêu tả cho ký tự “1” là “31”,… Mặc dù ban đầu hơi khó hiểu, quy ước này được sử dụng nhất quán trong suốt tiêu chuẩn như là tiêu chuẩn mô tả hệ thập lục phân và hệ nhị phân. Để phân biệt nó người ta gọi là “(ASCII)”.

Tập tin PERMIT.TXT sẽ được cung cấp qua các phương tiện phần cứng hoặc sử dụng dịch vụ trực tuyến theo quy trình vận hành của Data Servers. Các thủ tục này có sẵn cho Data Client khi mua một giấy phép.

Mỗi bản ghi Cell permit cũng chứa các trường bổ sung được cung cấp để hỗ trợ hệ thống OEM quản lý các tập tin giấy phép của Data Client từ nhiều Data Servers (xem phần 4.3.3).

Data Client có thể chứa một giấy phép để truy cập ENC bằng cách cung cấpUserpermit duy nhất của họ cho Data Server (xem phần 4.2). Data Server có thể trích xuất HW_ID từ Userpermit bằng cách sử dụng M_KEY của Data Client và tạo ra các Cell Permit riêng biệt dựa trên giá trị này. Định dạng của bản ghi Cell Permit được mô tả dưới đây trong phần 4.3.2 & 4.3.3.

Vì Cell Permit được phát hành cho một HW_ID riêng biệt, do vậychúng không được chuyển giao giữa các hệ thống của Data Client. Phương pháp này liên kếtgiấy phép để hỗ trợ cài đặt các sản phẩmtrên CD được mã hóa,có thể được phân phối tới tất cả các Data Client đăng ký vào dịch vụ.

Hệ thống Data Client giải mã các Cell Permit sử dụng HW_ID được chỉ định lưu trữ bảo mật bằng thiết bị phần cứng hoặc phần mềm. Các Cell key được giải mã sau đó có thể được sử dụng bởi hệ thống để giải mã các cell ENC. Từ đó, một số Data Servers có thể tạo tập tin giấy phép cho các ENC trong dịch vụ của họ, đó là trách nhiệm của hệ thống Data Client để quản lý các tập tin giấy phép từ một số Data Servers.

CHÚ Ý:Data Server nên tiếp tục cung cấp cả hai loại giấy phép (ENC.PMT & PERMIT.TXT) như được miêu tả trong S-63 phiên bản 1.0. Điều nàynên tiếp tục cho đến thời gian mà nó có thể được xác định rằng sự thiếu tập tin ENC.PMT sẽ không ảnh hưởng đến an toàn sử dụng của các hệ thống cũ hơn. Khoảng thời gian cần thiết cho điều này được thỏa thuận giữa tất cả thành phần tham gia. **OEM** phải đảm bảo thực hiện đầy đủ trong hệ thống phần mềm trong ECDIS của họ có khả năng hợp nhất các giấy phép từ nhiều Data Server mà không mất thông tin giấy phép bằng cách chỉ sử dụng tập tin PERMIT.TXT.

4.3.1 Tập tin Permit (PERMIT.TXT)

Các Cell Permit luôn được cung cấp trong tập tin gọi là PERMIT.TXT, tên tập tin luôn được cung cấp dạng chữ viết hoavới các ký tự chữ cái chứa trong tập tin.Tập tin này được mã hóa đầy đủ dạng ASCII[4] và gồm 3 phần như sau:

Phần	Miêu tả
Header	Phần này bao gồm tập tin tạo thành ngày tháng và định dạng phiên bản
:ENC	Giấy phép ENC (chính thức) từ Data Server được liệt kê trong phần này.
:ECS	Giấy phép ENC (không chính thức) từ Data Server có thể được liệt kê trong phần này.

Data Server hướng dẫn cách để các tập tin Permit sẽ có sẵn trên thiết bị phần cứng hoặc trên dịch vụ trực tuyến.Bảng dưới đây xác định nội dung và định dạng cho mỗi phần trong tập tin Permit được tách biệt bởi "dòng mới [NL]".

[4] OEM nên biết rằng tất cả các tập tin ASCII được tạo ra bởi lược đồ có thể chứa sự không rõ ràng ở cuối dòng được đánh dấu như là CR hoặc CRLF và sẽ đề cập tới những điều này.

4.3.2 Định dạng Header trong tập tin Permit

Bảng sau đây định nghĩa nội dung và định dạng phần Header trong tập tin Permit.

Phần	Tên trường	Giá trị
Ngày và giờ	**: DATE**	Tên trường, ngày và giờ được tách biệt bởi ký tự khoảng trống (SP <h20>).Ngày được cung cấp dạng YYYYMMDD và giờ được cung cấp dạng HH:MM sử dụng đồng hồ 24 giờ. Ví dụ: **:DATE** 20050809 11:11.
Phiên bản Meta Permit	**: VERSION**	Dạng số nguyên từ 1 đến 99. Nó sẽ tăng thêm 1 cho mỗi phiên bản mới của định dạng tập tin permit trong Chi tiết kỹ thuật. Ví dụ: S-63 Ấn bản 1.1 xác định giá trị là "2". Nghĩa là VERSION 2.
Kiểu Cell Permit	**: ENC**	Trường chứa định nghĩa các Permit có sẵn trong một phân phối giấy phép ENC từ Data Server. Trường được nhận biết bằng nhãn sau ở dạng chữ hoa **:ENC.**
Kiểu Cell Permit	**: ECS**	Trường chứa định nghĩa Meta Permit có sẵn trong phân phối giấy phép ECS từ Data Server. Trường được nhận biết bằng nhãn sau đây dạng chữ hoa**: ECS.**

Ví dụ:

:DATE 20080809 11:11
:VERSION 2
:ENC
Danh sách Cell Permit được cấp giấy phép cho ENC chính thức.
:ECS
Danh sách Cell Permit được cấp giấy phép cho các sản phẩm véc-tơ.

4.3.3 Trường trong Bản ghi Permit

Bản ghi Cell Permit bao gồm những trường sau đây được tách biệt bởi dấu phẩy:

Trường	Giá trị
Cell Permit	Được định nghĩa trong phần 4.3.4 và 4.3.5
Service Level Indicator (Chỉ số mức độ dịch vụ)	0 cho việc mua giấy phép dài hạn 1 cho việc mua giấy phép ngắn hạn.
Edition Number - Số phiên bản (tùy chọn)	DSID-EDTN là số phát hành của cell ENC (chỉ sử dụng cho Data Server).
Data Server ID	Đây là hai ký tự chữ cái được phát hành bởi SA.
Comment	Đây là trường văn bản còn trống để chú thích lên Cell Permit,…

CHÚ Ý: Trường "Số phiên bản [tùy chọn]" không còn là một yêu cầu bắt buộc trong S-63 Ấn bản 1.1.**OEMs** triển khaitheo Ấn bản 1.1 nên không còn xây dựng phụ thuộc vào hệ thống của họ để kiểm tra mối quan hệ giữa số phiên

bản của ENC và Cell key được sử dụng để mã hóa nó. Data Clients sẽ chỉkiểm tra đểxem xét khi có 1 Cell key hợp lý trong chuỗi permit. Data Server sẽ tiếp tục hỗ trợ các tập tin PERMIT.TXTtrong Ấn bản 1.0 cho đến khi thời gian cho ấn bản này được xác định là không còn được yêu cầu.

4.3.4 Định nghĩa Cell Permit

Bảng sau đây định nghĩa các trường chứa trong Cell Permit với sự định nghĩa mục đích của mỗi trường

Trường	Mục đích
Tên Cell	Tên Cell cho phép hệ thống Data Client liên kết chính xác khóa mã hóa tới các tập tin ENC được mã hóa tương ứng.
Ngày hết hạn	Ngày mà giấy phép của Data Client hết hạn, hệ thống phải ngăn ngừa các cell ENC mới, các phiên bản mới hoặc các bản cập nhật được tạo ra sau ngày này được cài đặt.
Cell Key 1 được mã hóa (ECK1)	ECK1 chứa khóa giải mã cho phiên bản hiện tại của Cell ENC.
Cell Key 2 được mã hóa (ECK2)	ECK2 chứa khóa giải mã được sử dụng khi Cell Key tiếp theo được lặp lại. Sắp tới, key được chứa trong Cell Permit cho phép Data Server định kỳ thay đổi Cell Key không cùng một lúc bằng cách phát hành các Cell Permit mới cho tất cả các Data Client.
Check Sum (CRC)	Giá trị này được cung cấp để bảo vệ khỏi sự tác động hoặc sự sửa đổi làm sai lệch ngẫu nhiên.

4.3.5 Định dạng Cell Permit

Cell Permit được viết dạng ASCII với định dạng và độ dài trường bắt buộc như sau:

Trường	Ký tự	Định dạng
Cell Name	8	Một chuỗi chữ-số tuân theo quy ước được định nghĩa trong S-57 Ấn bản 3.1, Phụ lục B phần 5.6 cho tên cell ngoại trừ phần mở rộng tên tập tin. Ví dụ: NO4D0613
Expiry Date(Ngày hết hạn)	8	Một chuỗi số chứa ngày hết hạn giấy phép cho mỗi ENC ở định dạng YYYYMMDD. Ví dụ: 20000830 (30 tháng 8 năm 2000).
ECK1 & ECK2[5]	16	Cell Key là 5 byte các số ngẫu nhiên - miêu tả bằng số Hex của chúng được mã hóa bằng cách sử dụng thuật

[5] Cell Permit chứa 2 trường để cung cấp cho hệ thống Data Client với các Cell Key cần thiết để giải mã các tập tin ENC cụ thể. Các trường này có thể chứa hai Cell Key giống nhau hoặc hai cell key khác nhau và có thể khác nhau giữa các Data Server. Một số Data Server có thể muốn tăng các cell key chỉ đến khi lược đồ bảo vệ có các thỏa hiệp khác ưu tiên để định kỳ tăng theo thủ tục dịch vụ của họ. Kỹ thuật để Data Server cung cấp các key này được miêu tả chi tiết trong phần 9.5.1. OEM nên lưu ý rằng

Trường	Ký tự	Định dạng
		toán Blowfish và sau đó được biểu diễn theo hệ thập lục phân trong Permit. Chú ý: Thuật toán mã hóa Blowfish tạo ra dữ liệu được mã hóa để đệm thêm bội số của 8 byte vào chiều dài. Điều này có nghĩa là các Cell key được mã hóa hiện tại dài 8 byte, mặc dù dạng không mã hóa chúng chỉ dài 5 byte (10 số Hex). Ví dụ: ECK1: **BEB9BFE3C7C6CE68** ECK2:**B16411FD09F96982**
ENC Permit Checksum	16	Chứa Check Sum được mã hóa cho Cell Permit. Nó được mã hóa sử dụng thuật toán Blowfish với HW_ID riêng biệt của Data Client và là một số 8 byte. Check sum này được mã hóa khác với Check sum không được mã hóa của User Permit. Ví dụ như Check Sum ENC trong ví dụ bên dưới là: **795C77B204F54D48**

Ví dụ: Trường Cell Permit

NO4D061320000830BEB9BFE3C7C6CE68B16411FD09F96982795C77B204F54D48

Tên Cell	Ngày hết Hạn	Dạng mã hóa của Cell Key 1	Dạng mã hóa của Cell Key 2	Check Sum (CRC)

Ví dụ: Bản ghi Cell Permit

Data Server ID

Cell Permit

Chỉ số mức độ dịch vụ

NO4D061320000830BEB9BFE3C7C6CE68B16411FD09F96982795C77B204F54D48,0,5,PM,[Comment]

Số ấn bản (nếu có)

4.3.6 Bổ sung tập tin License (tùy chọn)

Data Server có thể bao gồm một tập tin bổ sung với tập tin PERMIT.TXT để nhận biết cấp phép và cung cấp thông tin liên quan đến hệ thống ID[6]. Tập tin này được đặt tên là **.LIC, trong đó ** là miêu tả ID của Data Server.

Hệ thống Data Client có thể truy cập tới tập tin này (nếu có) để hiển thị thông tin người dùng và cung cấp thông tin Userpermit.

Tập tin này chứa một bản ghi duy nhất với các trường sau:

---

bất kỳ phần phụ thuộc trên số ấn bản nên được gỡ bỏ khỏi hệ thống của họ trong Ấn bản 1.1 của Lược đồ.

[6]Sẽ rất hữu ích khi xử lý các truy vấn Data Client để có thể truy cập nhanh tới thông tin của khách hàng như thông tin cấp giấy phép và ID nhà sản xuất. Data Client có thể cung cấp tập tin này với truy vấn để tăng tốc độ thời gian đáp lại.

Trường ID	Ký tự	Ghi chú
Bên được cấp phép	40	Tên của công ty hoặc cá nhân ký vào giấy phép.
Tên tàu	40	Tùy chọn. Trường này có thể để trống.
Fixed Site #1	240	Tên và địa chỉ của công ty. Trường này chứa văn bản định dạng tự do được sắp xếp trong các trường con6x40 byte. Văn bản sẽ không vượt quá ranh giới của các trường con.
Tên hệ thống máy chủ	40	Ví dụ: Main, Backup,…
User Permit	28	Giấy phép người dùng - hệ thập lục phân (Hex).
Loại giấy phép	40	Chỉ số dịch vụ, ví dụ Dịch vụ ENC của Primar Stavanger.
Dữ liệu HO	36	Dữ liệu sử dụng cho cơ quan thủy đạc/ đại lý/nhà phân phối.

Tổng số: 464 bytes

5 XÁC NHẬN DỮ LIỆU

5.1 Giới thiệu về Xác nhận dữ liệu và kiểm tra tính toàn vẹn

Kỹ thuật chữ ký số được dùng trong Lược đồ S-63 sử dụng tiêu chuẩn thuật toán và cơ chế trao đổi khóa được dùng rộng rãi. Chữ ký số S-63 sử dụng thuật toán khóa công khai bất đối xứng trong lược đồ PKI- như một nền tảng để không phá vỡ ràng buộc tập tin dữ liệu với định danh của nhà phát hành.

Lược đồ dựa trên sự mã hóa bất đối xứng[7] của một Check Sum trong một tập tin dữ liệu.Bằng cách xác minh chữ ký dựa vàokhóa công khai (public key) của nhà phát hành và cũng xác minh khóa công khai của nhà phát hành dựa vào sự nhận biết cấp cao nhất cho người sử dụng để đảm bảo danh tính của người ký.Chi tiết về chữ ký số vượt quá phạm vi của tài liệu này và người đọc nên tham khảo thêm tài liệuTiêu chuẩn về chữ ký số (DSS), FIPS Pub 186(www.itl.nist.gov/div897/pubs/fip186.htm) để được giải thích chi tiết và dễ tiếp cận hơn.

Lược đồ gồm 3 giai đoạn:

1) Nhà quản trị lược đồ (SA) xác minh danh tính của nhà cung cấp thông tin ENC và cung cấp cho nhà cung cấp cùng với dữ liệu để cho phép họ ký vào dữ liệu ENC.
2) Data Server (Ví dụ RENC hoặc VAR) phát hành dữ liệu ENC được ký với mã định danhcủa chúng (và được kiểm tra xác nhận bởi SA).
3) Sau đóData Client xác minh về định danh của Data Server (bởi nó liên quan đến SA) và sự toàn vẹn của dữ liệu ENC.

CHÚ Ý: QUY TRÌNH XÁC NHẬN ENC

1. Tập tin Khóa chung (Public Key) và Khóa tự ký (SSK - Self Signed Key) của Data Server được gửi đến SA để phê chuẩn.

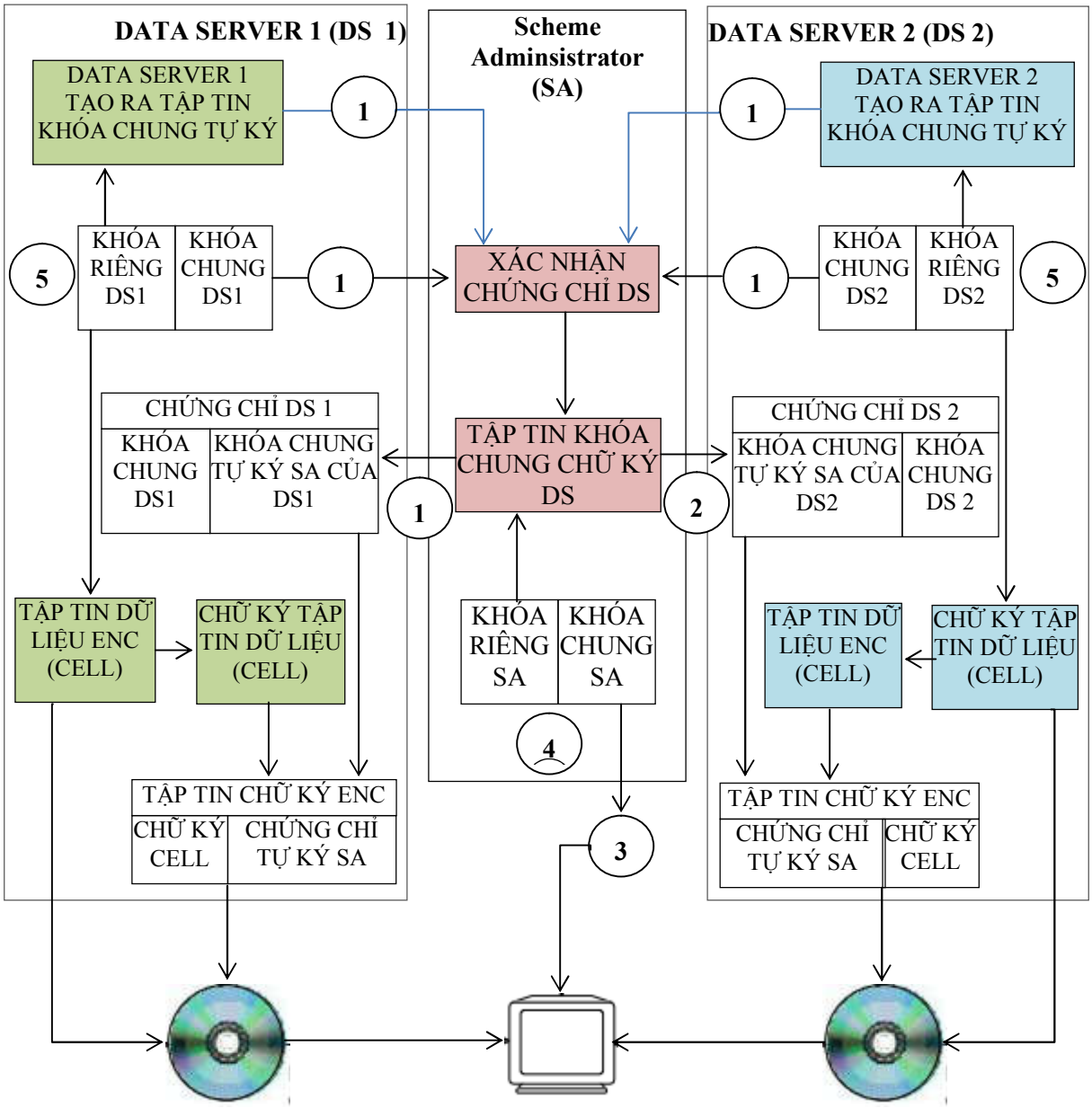
2. Nếu SA chấp nhận phê chuẩn, SA sẽ tạo khóa tự ký SSK kèm theo khóa riêng (Private Key)để tạo một Chứng chỉ Data Server được SA ký.

3. Khóa chung (Key Public)của SA được phân phối rộng rãi và được cài đặt độc lập trên hệ thống OEM.

4. Cặp khóa chung (Key Public) và khóa riêng (Key Private)của SA phải khác với tất cả các Data Server khác.

5. Tất cả Key Public và Key Private của Data Server phải khác nhau và phảikhác với SA.

[7]Mã hóa bất đối xứng dựa trên thuật toán mã hóa và giải mã tiến hành với các khóa mã hóa khác nhau.Vì vậy, một người có thể mã hóa dữ liệu và cung cấp khóa giải mã cho những người khác để giải mã nó. Các khóa này được gọi là “private key” và “public key”, gọi chung là một cặp khóa.



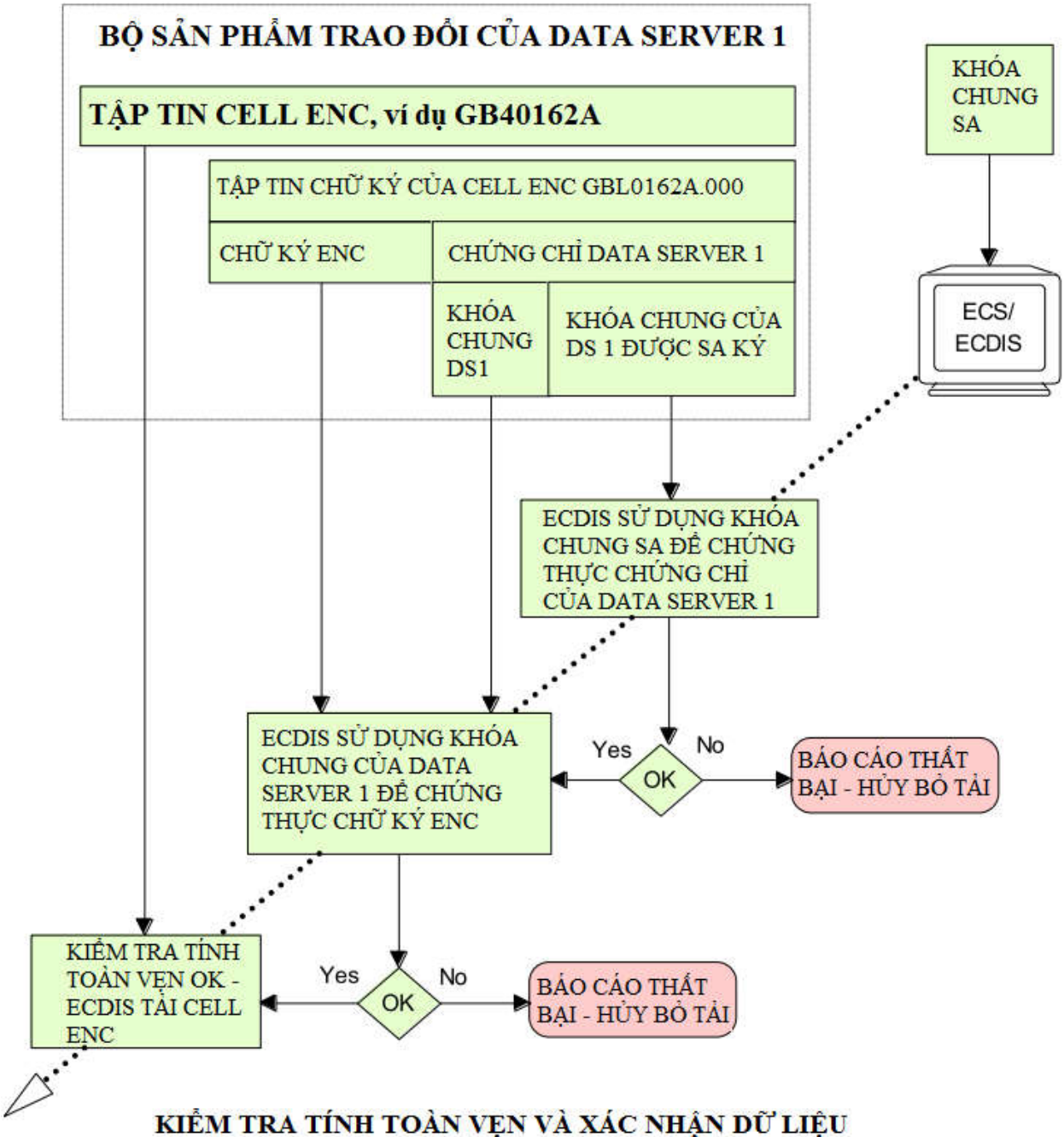
QUY TRÌNH XÁC NHẬN ENC

CHÚ Ý - XÁC NHẬN DỮ LIỆU VÀ KIỂM TRA TÍNH TOÀN VẸN DỮ LIỆU

Nếu ECS/ECDIS sử dụng phương thức được miêu tả ở trên, và nếu cặp Khóa của SA khác với cặp Khóa của Data Server, khi đó ECS/ECDIS có khả năng xác nhận và phê chuẩn các ENC từ Data Server 2 (hoặc bất cứ Data Server khác trong lược đồ) bằng cách sử dụng Khóa chung SA.

1 Xác nhận: ECS/ECDIS sử dụng Public Key của SA, trước đó được cài đặt độc lập trên CD, để kiểm tra một phần chứng chỉ của tập tin chữ ký nhằm xác nhận rằng Public Key của nhà cung cấp trong chứng chỉ là hợp lý. Như vậy, Data Server là thành viên hợp pháp của lược đồ.

2 Kiểm tra tính toàn vẹn: ECS/ECDIS sử dụng Public Key từ chứng chỉ để kiểm tra chữ ký củatập tin Cell ENC (dữ liệu).



KIỂM TRA TÍNH TOÀN VẸN VÀ XÁC NHẬN DỮ LIỆU

5.1.1 Sự xác minh SA

ECDIS cần có khả năng xác minh ENC có nguồn gốc hợp pháp. ECDIS làm điều này bằng cách đảm bảo Public Key của Data Server được cung cấp bên trong tập tin Chữ ký ENC có thể được xác nhận dựa vào Public Key của SA.

SA cung cấp chứng chỉ cho mỗi Data Server trong lược đồ; mỗi chứng chỉ là duy nhất, SA chỉ cấp 1 lần cho mỗi Data Server khi họ tham gia vào lược đồ.Đối với một chứng chỉ thu được, Data Server tạo ra một cặp khóa và cung cấp Public Key cho SA (như một chứng chỉ tự ký); SA (sử dụng cặp khóa hiện có của mình) sử dụng Private Key của mình để ký vào Public Key của Data Server. Kết quả là chứng chỉ chứa chữ ký Public Key của nhà phân phối.Chứng chỉ này sau đó được bao gồm bên trong tất cả các tập tin chữ ký của cell ENC và các bản cập nhật.

SA tạo ra nhiều Public Key và phổ biến rộng rãi tới cộng đồng ECDIS và các OEM nên cung cấp phương tiện để người sử dụng tải các dữ liệu độc lập này.

5.1.2 Toàn vẹn dữ liệu (Data Integrity)

Sau khi nguồn gốc Bộ sản phẩm đổi ENC được xác nhận, ECDIS sẽ kiểm tra tính toàn vẹn dữ liệu bằng cách phê chuẩn tập tin chữ ký được cung cấp cho mỗi ENC bởi Data Server.

Data Server tạo ra một tập tin chữ ký cho mỗi Cell bao gồm 2 phần sau:

- Chữ kýcủa tập dữ liệu [được tạo bằng cách sử dụng Private Key của Data Server, một nửa cặp khóa của Data Server (về cơ bản đây là một Checksum được mã hóa của dữ liệu) và khác nhau cho mỗi Cell].
- Chứng chỉ Data Server của họ (vẫn không thay đổi)

ECDIS sử dụng Public Key của Data Server có trong chứng chỉ để phê chuẩn tập tin dữ liệu chữ ký (nó giải mã tập tin dữ liệu chữ ký này và đối chiếu với Checksum tương ứng dựa vào Cell ENC). Nếu việc kiểm tra xác nhận thành công, chứng tỏ dữ liệu ENC là toàn vẹn và tính đồng nhất của Data Server bên trong chữ ký cell được xác nhận bởi SA.

5.2 Chứng chỉ số (sự xác nhận SA)

Chứng chỉ số là tập tin số được phát hành bởi một cơ quan cấp chứng chỉ. Họ ràng buộc Public Key nhất định với thông tin khác của một cá nhân hoặc tổ chức.Các chứng chỉ giúp ngăn chặnngười khác sử dụng Public Key giả mạo để mạo danh người khác.Lược đồ sử dụng một loạt các chứng chỉ, mỗichứng chỉ được xác nhận cho tới khi tất cả các bên xác nhận chắc chắn.Chứng chỉ SA được sử dụng bởi IHO sẽ là chứng chỉ tự ký[8]và là **chứng chỉ gốc** cho lược đồ.

SA sẽ phát hành chứng chỉ số tới tất cả Data Server được phê chuẩn bằng cách ký vào tập tin Public Key đã được xác minh của Data Server.Danh sách sau đây gồm các thao tác được thực hiện để phát hành chứng chỉ số.

Tạo Lược đồ

- SA tạo một cặp Public Key và Private Key duy nhấtở mức cao nhất.

Thiết lập của Data Server:

- Data Server tạo một cặp Public Key và Private Key duy nhất.

[8]Public Key của SA được ký bằng cách sử dụng Private Key của SA.

- Data Server tạo một Khóa tự ký (SSK) bằng cách ký vào tập tinPublic Key của chính nó với Private Key của chính nó.

- Data Server cung cấp SSK tới SA bằng một phương pháp đáng tin cậy.

- SA xác minh SSK của Data Server bằng cách sử dụng Public Key của Data Server.

- SA ký xác nhận tập tin Public Key của Data Server bằng cách sử dụng Private Key của SA.

- SA cung cấp cho Data Server với Chứng chỉ Data Serverđược ký bởi SA duy nhất của chính nó.

Tạo ra tập dữ liệu được ký:

- Data Server xác nhận chứng chỉ kết quảbằng Public Key củaSA (được cung cấp riêng).

- Data Server lưu trữ chứng chỉ đã được xác nhận và sử dụng nó để tạo các tập tin chữ ký ENC.

Định dạng của các tập tin, các chứng chỉ và chữ ký khác nhau được miêu tả chi tiết hơn trong phần 5.4.

CHÚ Ý: Public Key của SA được tạo sẵn cho tất cả các bên liên quan, ví dụ Data Server, Data Client và OEM, bằng một sốcách như Web, e-mail,…

5.2.1 Public Key của SA

Lược đồ yêu cầuPublic Key của SA được cài đặt trên hệ thốngData Client độc lập với Bộ sản phẩm trao đổi ENC. Điều này có thể được cài đặt sẵn bởi OEM. Tuy nhiên, hệ thống Data Client phải có phương pháp cài đặt một Public Key mới[9]trên hệ thống trong trường hợp một Public Key mới được phát hành bởi SA.

Sau khi người dùng cài đặt một Chứng chỉ SA hoặc Public Key mới, hệ thống phải xác nhận chúng đã được cài đặt. Nếu cài đặt một chứng chỉ SA mới (IHO.CRT) thì hệ thống phải thông tin cho người dùng như sau:

"***Một Chứng chỉ SA mới (Public Key) đã được cài đặt, điều này là hợp lệ để đăng ký ngày hết hạn hoặc trừ khi SA phát hành một chứng chỉ mới vì lý do an ninh***".

Nếu cài đặt một SA Public Key mới (IHO.PUB), hệ thống phải thông báo cho người dùng như sau:

"***Một Public Keymới củaSA đã được cài đặt, điều này là hợp lệ cho đến khi SA đều đặn phát hành Public Key mới hoặc trừ khi nó được phát hành vì lý do an ninh***".

Nên khi hệ thống báo một lỗi xác nhận trong suốt quá trình tải lên, nó sẽ báo động cho người dùng rằng SA có thể đã thay đổi Public Key.Vì vậy, thông điệp cảnh báo phải được hiển thị để giải thích lý do này như sau:

"***SSE 06 – Chứng chỉ SA/Public Key không hợp lệ.SA có thể đã phát hành một Public Key mới hoặc ENC có thể sinh ra từ một dịch vụ khác. Có thể thu về một SA Public mới từ nhà phân phối của bạn hoặc từ trang web của IHO***".

[9]Nó được biết trước Data Server sẽ cung cấp bộ sản phẩm trao đổi độc lập này để đúng với dữ liệu đã được xác minh tương phản với Public Key mới.

5.2.2 Data Server mới

IHO phối hợp với DPSWG sẽ thiết lập danh tínhcho bất kỳ tổ chức hoặc công ty thương mại nào muốn tham gia vào lược đồ bảo vệ như một Data Server. Nếu SA thu hồi Chứng chỉ Data Server, nó sẽ thông báo cho tất cả các Data Server và Nhà sản xuất về sự thay đổi.

5.3 Chữ ký số (để xác minh tính toàn vẹn dữ liệu)

Chữ ký số là một chữ ký điện tử có thể được sử dụng để xác nhận danh tính của người gửi tin nhắn hoặc người ký vào tài liệu, để đảm bảo nội dung ban đầu của tin nhắn được gửi là không thay đổi. Chữ ký số dễ dàng đem theo, dễ dàng kiểm chứng và không thể giả mạo.

Các văn phòng thủy đạc hoặc tổ chức Data Server khác (ví dụ RENC/VAR) cũng có thể sử dụng chữ ký số nhằm duy trì nguồn gốc và tính toàn vẹn giữa chúng trong việc cung cấp các thông tin ENC. Mỗi tập tin ENC (cả bản gốc và bản cập nhật) sẽ luôn có một tập tin chữkýsố duy nhất liên kết với nó. Không một tập tin nào khác trong một Bộ sản phẩm trao đổi ENC đã mã hóa có chữ ký số.

LƯU Ý:Một Bộsản phẩm trao đổi có thể chứa chữ ký số được phát hành bởi các Data Server khác nhau và do đó mỗi tập tin ENC phải được xác thực một cách riêng lẻ.

5.3.1 Tổng quan về kỹ thuật Chữ ký số

Xác thực dữ liệu được cung cấp bằng cách sử dụng chữ ký số phù hợp với Tiêu chuẩn chữ ký số (DSS- Digital Signature Standard).DSS sử dụng thuật toán bảo mật Hash (SHA-1- Secure Hash Algorithm) [3] để tạo ra một thông điệp tóm tắt (hash). Thông điệp tóm tắt này sau đó là đầu vào cho thuật toán chữ ký số (DSA-Digital Signature Algorithm) để tạo ra các chữ ký sốbằng cách sử dụng một thuật thuật toán mã hóa bất đối xứng và "Private Key" của một cặp khóa. Thuật toán bất đối xứng được mã hóa bằng cách sử dụng "Private Key" của cặp khóavà chỉ có thể được giải mã bằng cách sử dụng "Public Key" của cặp khóa.

Việc mã hóa thông điệp tóm tắt với Private Key đảm bảo cho bất kỳ người nào có Public Key (như tên của nó đề nghị có thể được công bố) có thể giải mã và xác nhận thông điệp tóm lược. Thông tin thêm về Chữ ký số và cách sử dụng chúng có thể tham khảo từ trang web của IHO (http://www.iho.int).

5.3.2 Quy ước đặt tên tập tin chữ ký ENC

Tập tin chữ ký số sẽ phù hợp với tên tập tin cell, ngoại trừ các mã dùng cho mục đích dẫn đường, chữ số 1-6 sẽ được thay thế bởi các chữ I-N.

Nhìn chung:

Tập tin ENC: CC[1-6]XXXXX.EEE (Xem S-57 Phụ lục B1)

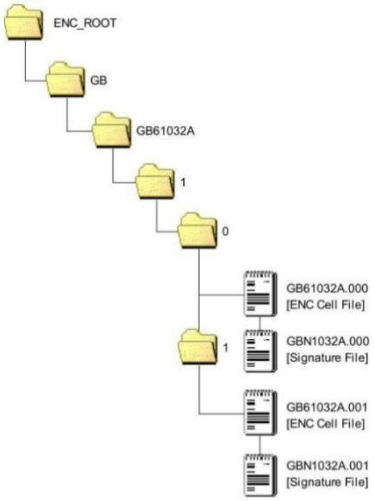
Tập tin Chữ ký: CC[I-N]XXXXX.EEE

Mục đích hàng hải	Ký tự chữ ký
1. Đại dương	I
2. Ngoài khơi	J
3. Ven bờ	K
4. Tuyến luồng	L
5. Vùng nước trước cảng	M
6. Vùng neo	N

Ví dụ:

Tập tin Cell: GB100001.000 sẽ có tập tin chữ ký đặt tên làGBI00001.000

Tập tin Cell: GB61032A.002 sẽ có tập tin chữ ký đặt tên làGBN1032A.002



VỊ TRÍ TẬP TIN CHỮ KÝ SỐ ENC

5.3.3 Lưu trữ tập tin chữ ký ENC

Tập tin chữ ký ENC phảilà duy nhất, thuộc tập tin dữ liệu ENC cụ thể như đã nêu trong mục 5.3.2 ở trên. Tập tin chữ ký số sẽ luôn được đặt trong cùng thư mục với tập tin Cell ENC liên quan đến nó, như minh họa phía dưới.

5.4 Định dạng tập tin xác nhận dữ liệu

Có một số tập tin liên kết với quá trình xác nhận trong Lược đồ bảo vệ dữ liệu S-63. Trong số này có tập tin chứng chỉ và chữ ký như đã được miêu tả trong phần 5.2 và 5.3 và Private Key, Public Key được tạo ra để ký và xác thực chúng. Mặc dù điều này có thể được bắt nguồn một cách độc lập từ các bộ phận cấu thành khác nhauchứa trong mỗi tập tin chia sẻ các yếu tố chung luôn được định dạng theo cùng một cách. Bảng sau đây liệt kê các tập tin là nền tảng cho việc xác thực ENC được mã hóa theo S-63. Bảng này cũng xác định các thành phần tham gia lược đồ tạo ra chúng:

Kiểu tập tin	**Nhà quản trị lược đồ**	**Data Server**
Tập tin PQG	✓	✓
Khóa riêng (Tập tin X)	✓	✓
Khóa chung (Tập tin Y)	✓	✓
Chứng chỉ X509 v3	✓	✗
Khóa tự ký (SSK)	✗	✓
Chứng chỉ	✓	✗
Chữ ký	✗	✓

5.4.1 Thành phần tập tin

Bao gồm 2 phần, phần tiêu đề và một chuỗi dữ liệu. Bảng sau đây liệt kê

các thành phần có thể tạo nên một tập tin cụ thể, chứng chỉ hoặc chữ ký:

Yếu tố	Tiêu đề	Chuỗi dữ liệu
R	// Phần chữ ký R:	10 khối, mỗi khối 4 ký tự
S	// Phần chữ ký S:	10 khối, mỗi khối 4 ký tự
p	// BIG p	32 khối, mỗi khối 4 ký tự
q	// BIG q	10 khối, mỗi khối 4 ký tự
g	// BIG g	32 khối, mỗi khối 4 ký tự
x	// BIG x	10 khối, mỗi khối 4 ký tự
y	// BIG y	32 khối, mỗi khối 4 ký tự

5.4.1.1 Định dạng thành phần tiêu đề và chuỗi dữ liệu:

Mỗi chuỗi dữ liệu:

- Bắt đầu bởi một dòng tiêu đề duy nhất. Các dòng tiêu đề được chỉ ra bởi 2 dấu gạch chéo đặt phía trước (//ASCII-0x2F2F), tiếp theo sau đó là một khoảng trống (SP ASCII 0x20) và các ký tự Tiêu đề dạng ASCII theo định dạng được mô tả bên dưới.
- Được biểu diễn trong văn bản ASCII bằng các số hệ thập lục phân (0-9, A-F).Các ký tự chữ cái phải viết hoa.
- Kết thúc bởi dấu chấm (.) (.ASCII 0x2E).
- Có một khoảng trống (ASCII SP 0x20) tách biệt từng nhóm 4 ký tự.
- Có một Carriage Return (ASCII CR 0x0D) và dòng mới (ASCII LF 0x0A) tại cuối mỗi chuỗi dữ liệu.

5.4.2Ví dụ về định dạng Tập tin, chứng chỉ và chữ ký

Phần sau đây bao gồm ví dụ về tất cả các tập tin khác nhau liên quan tới khía cạnh này của Lược đồ Bảo mật dữ liệu hải đồ điện tử(S-63).Việc giải thích chi tiết làm cách nào để các tập tin này được tạo ra sẽ được tóm lược ở cuối tài liệu này.

5.4.2.1Định dạng PQG

Các tham số PQG được tạo ra từ một chuỗi ký tự ngẫu nhiên và sau đó được sử dụng để tạo các thành phần X và Y, tức là cặp khóa Private Key/Public Key. Sau khi tạo xong bộ tham số PQG, nội dung của nó đượcchứa bên trong các thành phần X và Y (tức là cặp Private Key/ Public Key).

P, Q và G là các tham số dạng số học được sử dung trong Giải thuật Chữ ký số như đầu vào cho quá tình tạo khóa.Mỗi Data Server có thể sử dụng một bộ P, Q và G khác nhau hoặc sử dụng một tập hợp đã có sẵn có để tạo ngẫu nhiên một cặp khóa.Tiêu chuẩnChữ ký số [2] miêu tả nguồn gốc và quyền sử dụng của họ.

Ví dụ về định dạng PQG:

// BIG p
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.
// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.
// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.

5.4.2.2Định dạng X (Private Key)

Tập tin X có thể viết dược dạng ASCII theo định dạng sau:

// BIG p
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.
// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.
// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.
// BIG x
EBAF 2948 1485 7E7C 2F48 C7B2 9334 2F09 DA1A EB04.

5.4.2.3 Định dạng Y (Public Key của IHO hoặc của Data Server)

Public Key của cả SA và Data Server được cung cấp theo định dạng sau đây, lược đồ sử dụng Public Key DSA có độ dài 512 bit.

// BIG p
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.
// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.
// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.
// BIG y
444B BA17 1758 0DAF 71AB 52A5 6CCA 8EAB 4C51 E970 0E37 B17B BB46 C0B9 4A36 F73F
0244 7FBD AE5B 7CA9 38705AB9 E9EE 471C E7B0 1004 6DF1 3505 42B3 0332 AE67 69C6.

5.2.4 Định dạng Chứng chỉ số SA (X509v3)

Chứng chỉ số SA sẽ có trong định dạng X509v3 [4] và miêu tả một Public Key DSA có chiều dài 512 bit. Chứng chỉ số SA có sẵn trong tập tin được gọi là IHO.CRT.Tập tin IHO.CRT có trong trang web IHO tại http://www.iho.int.

Tất cả Data Server cung cấp dịch vụ ENC bao gồm cả chứng chỉ SA để tham chiếu đến thư mục gốc của phương tiện lưu trữ (ví dụ: D:\IHO.CRT trên CD-ROM) nhưng như đã nêu trong phần 5.2.1, việccài đặt chứng chỉ SAlên hệ thốngData Client nên thực hiện độc lập. Việc kiểm tra tính hợp lệ của chữ ký SA dựa vào chữ ký ENC phải được thực hiện từ các phiên bản cài đặt độc lập của chứng chỉ SA.

Public Key của SA ở định dạng ASCII (trái với định dạng số nhị phân x509v3) cũng có sẵn trong trang web http://www.iho.int của IHO (định dạng được miêu tả trong phần 5.4.2.3).

5.4.2.5 Định dạng Khóa tự ký (SSK)

Đây là định dạng mà Data Server sử dụng để ký vào Public Key của chính nó trước khi gửi tới để SA ký. Chữ ký là chữ ký của toàn bộ tập tin Public Key (ví dụ: các tham số PQG và Y).

// Chữ ký phần R:
752A 8E5C 3AF5 6CCD 7395 B52E F672 E404 554F AAB6.
// Chữ ký phần S:
1756 E5C0 F4B6 BC90 4EC6 5F94 DF93 3ADF 68B8 86C4.

Thành phần chữ ký duy nhất
Chữ ký Data Server (DS) cho Public Key DS

// BIG p
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.
// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.
// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.
// BIG y
444B BA17 1758 0DAF 71AB 52A5 6CCA 8EAB 4C51 E970 0E37 B17B BB46 C0B9 4A36 F73F
0244 7FBD AE5B 7CA9 3870 5AB9 E9EE 471C E7B0 1004 6DF1 3505 42B30332 AE67 69C6.

Public Key của Data Server

Tập tin Public Key của Data Server

Chữ ký SA đượcxác minh bởi SA dựa vào Public Key được DS cung cấp.

5.4.2.6. Định dạng tập tin chứng chỉ Data Server được SA ký

Đây là định dạng tập tin được sử dụng bởi SA khi SA phát hành một tập tin Chứng chỉ Data Server. SA cũng sử dụng Public key DSA có độ dài 512 bít. Cặp R & S được chép lại thành tập tin chữ ký ENC của Data Server.

// Chữ ký phần R:
8FD6 2AC7 27D2 8D0B CD27 BDF2 5CC6 9656 10E3 751F.
// Chữ ký phầnS:
3DE7 DA37 5A40 80FC 4203 5C6E 37DE A984 2A88 2BDC.

Thành phần chữ ký duy nhất. Chữ ký của SAcho Public Key của DS

// BIG p
D0A0 2D76 D210 58DA 4D91 BBC7 30AC 9186 5CB4 036C CDA4 6B49 4650 16BB 6931 2F12
DF14 A0CC F38E B77C AD84 E6A1 2F2A A0D0 441A 734B 1D2B E944 5D10 BA87 609B 75E3.
// BIG q
8E00 82E3 C046 DFE6 C422 F44C C111 DBF6 ADEE 9467.
// BIG g
B08D 786D 0ED3 4E39 7C6B 3ACF 8843 C3BF BAB1 A44D 0846 BB2A C3EE D432 B270 E710
E083 B239 AF0E A5B8 693B F2FC A03B 6A73 E289 84FF 8623 1394 996F 6263 0845 AA94.
// BIG y
444B BA17 1758 0DAF 71AB 52A5 6CCA 8EAB 4C51 E970 0E37 B17B BB46 C0B9 4A36 F73F
0244 7FBD AE5B 7CA9 3870 5AB9 E9EE 471C E7B0 1004 6DF1 3505 42B3 0332 AE67 69C6.

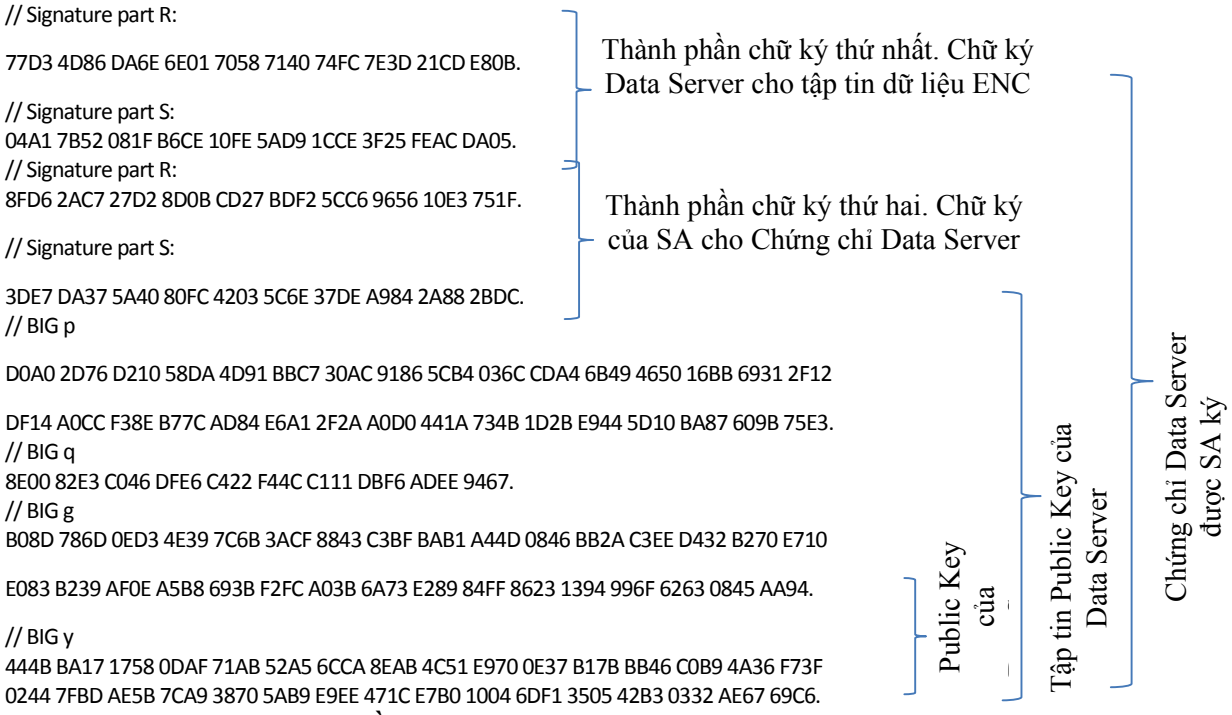
Public Key của Data Server

Tập tin Public Key của Data Server

Chứng chỉ Data Server được SA ký

5.4.2.7 Định dạng tập tin chữ ký ENC

Tập tin chữ ký phải chứa một cặp chữ ký và chứng chỉ. Tập tin với chỉmỗi chữ ký là không hợp lệcũng như không được chứngnhậnđể nhận dạng trong Data Server. Tập tin chữ ký số ENC có định dạng, cấu trúc và thứ tự như ví dụ sau:



Cặp chữ ký R&S đầu tiên được xác nhận bởi Public Key của Data Server.

Cặp chữ ký R&S thứ haiđược xác nhận bởi Public Key của SA lưu trữ trong ECS/ECDIS.

Cặp R và S thứ hai được sử dụng để xác nhận Chứng chỉ số của Data Server (các chuỗi p, q, g và y). Nếu xác nhận thành công, Public Key của Data Server (chuỗi y) có thể được giải nén và sử dụng để xác minh chữ ký số (cặp R và S thứ nhất) của dữ liệu ENC mã hóa.Điều này cho phép Data Client xác minh chứng chỉ số SA, để trích xuất Public Key của Data Server và để xác minh chữ ký số của dữ liệu ENC.

6 QUẢN LÝ DỮ LIỆU

6.1 Giới thiệu

Việc tải và nhập dữ liệu ENC vào hệ thống ECS/ECDIS phải được quản lý một cách cẩn thận.Điều này đặc biệt đúng khi cónhiềuData Server. Khi lược đồ mã hóa toàn bộ nội dung tập tin cell ENC (bản gốc và bản cập nhật), hệ thống OEM hạn chế quyền truy cập vào trường con nào đó trong tập tin cell ENC để quản lý nhập ENC vào hệ thống ECS/ECDIS SENC. Điều này dẫn đến việc khó bổ sung dữ liệu S-63 cũng như sửa đổi một tập tin S-57 hiện có, ví dụ tập tin CATALOG.031.

Cũng dễ nhận ra rằng, việc nhập một lượng lớn các ENC làm cho một số khía cạnhcủa S-57 không thực tế để triển khai, ví dụ: Bộ sản phẩm traođổi duy nhất được tách ra thành nhiều khối trung bình. Ví lý do này, phảithay đổi chiến lược tải và sử dụng thêm tập tin S-63 để quản lý tốt hơn việc cài đặt và tải các ENC qua nhiều bộ sản phẩm trao đổi.

Như đề cập trước đó, S-63 được thiết kế để triển khai trong trường hợp cónhiều nhà cung cấpdữ liệu. S-57 không có cơ chế phân biệt giữa các Bộ sản phẩm trao đổi ENC được cung cấp bởi các Data Server khác nhau và do vậy nó cần có trong phiên bản 1.1 của tiêu chuẩn này.

Các tập tin S-63 bổ sung chứa thông tin quan trọng, nếu được sử dụng đúng cách, có thể làm cho quá trình nhập S-57 hiệu quả và trực quan hơn cho Data Client.

Phương thức tải lên/nhập vào có thể được chia làm các quá trình sau:

- Quản lý nhập các Bộ sản phẩm trao đổi ENCriêng biệtvào Data Server bằng cách sử dụng ID của Data Server.
- Quản lý dịch vụ của Data Server nếu mở rộng qua nhiều Bộ sản phẩm trao đổi.
- Quản lý nhập các Cell ENC được cấp phép theo thứ tự, bằng cách bảo đảm cho tất cả cell ENC gốc và các cell ENC cập nhật tương ứng (nếu có) được nhập vào chính xác và theo trình tự.
- Quản lý nhập các tập tin văn bản và hình ảnh bằng cách duy trì mối quan hệ giữa chúng và các cell liên kết với chúng.

Bảng sau đây liệt kê các tập tin S-63 bổ sung và tập tin chỉnh sửa cùng với mục đích chính của chúng trong S-63.Các tập tin này và định dạng liên kết của chúng được mô tả chi tiết trong phần 6.2, 6.3 & 6.4.

Tập tin/ Trường	**Chức năng quản lý đầu tiên**
PRODUCTS.TXT	Được yêu cầu cung cấp các thông tin sau đây: 1. Ngày phát hành của tập tin Products đang cài đặt. 2. Danh mục tất cả các Cell sẵn có trong dịch vụ của Data Server. 3. Phạm vi của tất cả các Cell sẵn có trong một dịch vụ. 4. Ngày phát hành sau cùng của tất cả các cellsẵn có trong một dịch vụ (bao gồm cả các cell đã bị xóa). 5. Đích đến của Bộ sản phẩm trao đổi (cơ sở hoặccập nhật) nơi chứa tập tin cell ENC gốc (cấu hình ứng dụng EN). Đây có thể là một cell gốc, một phiên bản mới hoặc một tái bản.
SERIAL.ENC	Yêu cầu cung cấp các thông tin sau: 1. ID của Data Server 2. Số tuần và ngày phát hành Bộ sản phẩm trao đổi. 3. Kiểu Bộ sản phẩm trao đổi (gốc hoặc cập nhật) 4. Số Bộ sản phẩm trao đổi trong một dãy.
CATALOG.031 [CATD-COMT]	Được yêu cầu cung cấp thông tin ban đầu chứa trong trường DSID của tập tin cell để nhập đầy đủ, liên tục nội dung một Bộ sản phẩm trao đổi.

6.2 Lập danh sách sản phẩm ENC (PRODUCTS.TXT)

Tên tập tin PRODUCTS.TXT được cung cấp với mỗi Bộ sản phẩm trao đổi đã mã hóa và được lưu trữ trong thư mục có tên "INFO" trong thư mục gốc. Nó có cơ chế quản lý dữ liệu trong mộtdịch vụ ENC và trao đổi nó với dữ liệu chứa trong hệ thống SENC của Data Client.Cấu trúc và định dạng của tập tin này được miêu tả chi tiết hơn trong phần 6.2.1, 6.2.2, 6.2.3 & 6.2.4.

Có hai loại tập tin PRODUCTS.TXT, đó là "PARTIAL" và "FULL". Danh sách sản phẩm từng phần (partial) chứa tình trạng hiện tại của tất cả các

ENC trong một Bộ sản phẩm trao đổi duy nhất. Danh sách sản phẩm đầy đủ (Full) chứa tình trạng hiện tại của TẤT CẢcác cell trong dịch vụ của Data Server, tức là tất cả các Bộ sản phẩm trao đổi. Mặc dù thủ tục có thể khác nhau giữa các Data Server, một danh sách sản phẩm đầy đủ sẽ luôn được cung cấp với Bộ sản phẩm trao đổi cập nhật hàng tuần. Trong trường hợp Data Server phát hành một bộ đầy đủ CD nền (Base CD) mới (không được cập nhật hàng tuần), mỗi Base CD phải chứa đầy đủdanh sách sản phẩm của tất cả các ENC trong một dịch vụ.

LƯU Ý: OEMđảm bảo rằng hệ thống của họ có khả năng thực hiện lập danh sách sản phẩm "FULL" và "PARTIAL" (tham khảo phần 6.2.2). Base CD có thể chứa danh sách sản phẩm từng phần với các nội dung mà CD chứa.Các Update CD sẽ luônthực hiện đầy đủ danh sách sản phẩm của tất cả các ENC sẵn có trong dịch vụ của Data Server.

Giấy phép và thông tin ENC từ các Data Server khác nhau phải được lưu trữ độc lập trên hệ thống của nhà sản xuất.Tập tin SERIAL.ENC (xem phần 6.3) chứa ID của Data Server và sẽ được sử dụngtrong việckết hợp với danh sách sản phẩm được liên kết để nhận biết nguồn gốc dịch vụ.Danh sách sản phẩm mới nhất chứa tình trạng hiện tại của dữ liệu cell ENC trong một dịch vụ.Tập tin này được sử dụng để so sánh dữ liệu cell ENC sẵn có trong Bộ sản phẩm trao đổi với thông tin đã lưu trữ trong các SENCcủa OEM. Hệ thống OEM sau đó xác định dữ liệu mới sẵn có để nhập vào.

Khuyến cáo rằngOEM nên duy trì một bản sao danh sách sản phẩm mới nhất trên hệ thống để phản ánh trạng thái hiện tại của một dịch vụ riêng biệt.Để quản lý cả hai danh sách sản phẩm "FULL" và "PARTIAL", điều quan trọng là thông tin mới được gộp vào với dữ liệu lưu trữ hiện có và không bị ghi đè.

6.2.1 Cấu trúc tập tin Danh sách sản phẩm (Product List)

Nội dung của Danh sách sản phẩm sẽ được chia thành nhiều phần. Một tập tin Danh sách sản phẩm được mã hóa dạng ASCII và chứa 3 phần sau:

Phần	Mô tả
Tiêu đề (Header)	Chứa thông tin chung về loại Danh sách sản phẩm, ví dụ thời gian tạo, số phiên bản.
:ENC	Chứa tình trạng hiện tại của tất cả cell ENC/Update được cung cấp bởi Data Server.
:ECS	Chứa thông tin về hải đồ sốkhác được cung cấp bởi Data Server .

6.2.2 Tiêu đề của Danh sách Sản phẩm

Danh sách Sản phẩm luôn bắt đầu với một phần tiêu đề.Phần tiêu đề gồm một vài bản ghi.Mỗi bản ghi bắt đầu ở một dòng mới và kết thúc với các ký tự ASCII CR/LF như trong tập tin Chữ ký.

Phần Tiêu đề gồm các trường thông tin được quy định trong ví dụ và bảng dưới đây. Tất cả các trường là bắt buộc và luôn được xác định theo cùng thứ tự.

Trường	Tên trường	Giá trị
Ngày và giờ	:DATE	YYYYMMDD HH:MM Tên trường, ngày tháng và thời gian được ngăn cáchbởi một ký tự <dấu cách>. Ngày tháng được cung cấp dạng20060627 và thời giandạng09:00:00 sử dụng đồng hồ 24h.

		Ví dụ: **DATE 20060627 09:00:00**
Phiên bản Danh sách Sản phẩm	:VERSION	Số nguyên trong khoảng từ 1 đến 99. Số phiên bản tăng thêm 1 cho mỗi phiên bản mới của tậptin PRODUCT.TXT. S-63 Phiên bản 1.1 định nghĩa giá trị là '2'. Ví dụ: **:VERSION 2**
Nội dung	:CONTENT	"FULL" là bản sao đầy đủ của Danh sách Sản phẩm. "PARTIAL" là bản sao từng phần của Danh sách Sản phẩm. Mã được sử dụng để chỉ ra nếu tập tin Danh sách Sản phẩmchứa một bản sao đầy đủ hoặc bản sao từng phần của Danh sách Sản phẩm hoàn chỉnh. Ví dụ: **:CONTENT FULL**

Ví dụ:

:DATE 20061019 09:00:00
:VERSION 2
:CONTENT FULL

6.2.3 Mục 'ENC' củaDanh sách sản phẩm

Danh sách sản phẩm luôn chứa một mục ENC. Mục nàycó thông tin về trạng thái hàng hải hiện tại của tất cả các cell ENC chính thức và ENC cập nhật được hỗ trợ bởi Data Server.

Phần này sẽbắt đầu với một bản ghi*phần định danhENC*như định nghĩa sau:

Trường	**Tên trường**	**Giá trị**
Định danh mục ENC	:ENC	Không áp dụng

Mục ENC sau đó bao gồm các bản ghi lặp lại xác định tình trạng của mỗi ENC được hỗ trợ bởi Data Server. Định nghĩa của bản ghi này được xác định trong bảng sau:

Trường	**Giá trị**
Tên sản phẩm	Tên sản phẩm được quy định trongtrường con DSID-DSNM của S57 E3. Phần mở rộng tập tin luôn là 000. Ví dụ: **GB202400.000**
Ngày phát hành Base Cell (Hồ sơ ứng dụng EN)	YYYYMMDD Ngày này chỉ được sử dụng cho các tập tin Base Cell (tức là bộ dữ liệu mới, dữ liệu tái bản và phiên bản mới), không sử dụng cho Update Cell. Tất cả các bản cập nhật ngày này hoặc trước ngày này phải được áp dụng bởi nhà sản xuất. Các Cell bị xóa với số phiên bản "0" sẽ có ngày phát hành của bản cập nhật được sử dụng để xóa nó. Ví dụ: **20050222**
Số phiên bản Base Cell	Số phiên bản của Base Cell ENC [EN] là số nguyên từ 1 đến 999, giống với nội dung của SDID-EDTN trong S57e3. Trong trường hợp một cell bị xóa thì số ấn bản của sản phẩm sẽ thiết lập về "0", xem phần 6.2.3.1. Điều này cho phép hệ thống ECDIS nhanh chóng xác định các cell đã gỡ bỏ khỏi một Dịch vụ.
Ngày phát hành bản cập nhật mới nhất (cấu hình	YYYYMMDD Ngày mà bản cập nhật mới nhất của phiên bản cell ENC hiện tại đãđược phát hành. Trường này được sử dụng mỗi khi có một

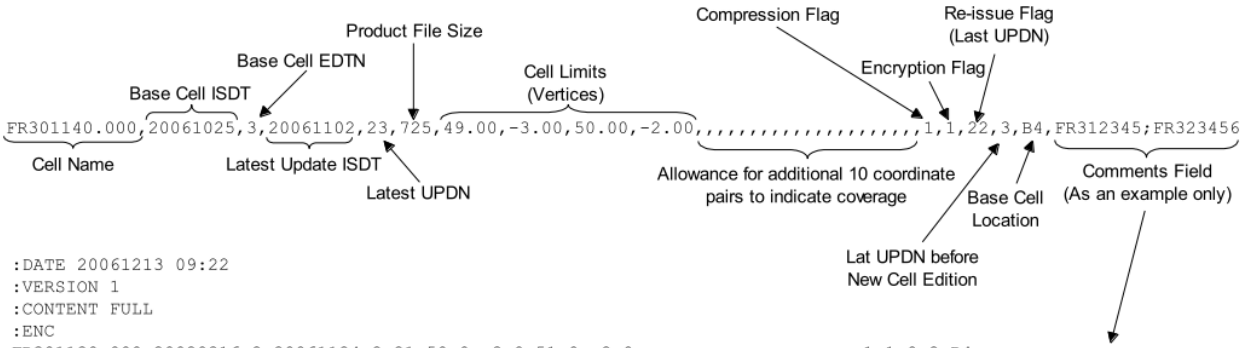
ứng dụng EN)	bản cập nhật hoặc một dữ liệu tái bản của cell.
Số bản cập nhật mới nhất	Dạng số nguyên từ 1 đến 999. Số cập nhật của thông báo cập nhật mới nhất được phát hành cho các phiên bản cell ENC. Giống với nội dung của DSID-UPDN. Để trống khi không có sẵn bản cập nhật cho phiên bản hiện tại của Base Cell. Chỉ được sử dụng cho các bản cập nhật và dữ liệu tái bản.
Dung lượng tập tin	Dạng số nguyên từ 1 đến 999999. Tổng dung lượng tập tin ở dạng Kilobytes cho tất cả tập tin được phát hành củasản phẩm. Bao gồm dung lượng của Base Cell, bản cập nhật và bất kỳtập tin ứng dụng text và hình ảnh.
Giới hạn vĩ độ cực Nam của Cell	Độ của vòng cung, phía Nam là âm. Vĩ độ cực Nam của độ phủ dữ liệu trong sản phẩm ENC. Ví dụ: **49.898773299986 (49º53´.93N)**
Giới hạn kinh độ cực Tây của Cell	Độ của vòng cung, phía Tây thì âm. Kinh độ cực Tây của độ phủ dữ liệu trong sản phẩm ENC. Ví dụ: **-1.927277300003 (001º55´.64W)**
Giới hạn vĩ độ cực Bắc của Cell	Độ của vòng cung, phía Nam thì âm. Kinh độ cực Bắc của độ phủ dữ liệu trong sản phẩm ENC. Ví dụ: **50.922828000014 (50º55´.37N)**
Giới kinh độ cực Đông của cell	Độ của vòng cung, phía Tây thì âm. Kinh độ cực Đông của độ phủ dữ liệu trong sản phẩm ENC. Ví dụ: **-0.000166700008 (000º00´.01W)**
10 tọa độ bao phủ dữ liệu	Tùy chọn. Độ của vòng cung, phía Nam và Tây là âm. 10 cặp tọa độ có thể được cung cấp để cho chỉ ra độ phủ dữ liệu trong cell ENC. Nó sẽ được cung cấp bằng cách lặp đi lặp lại cặp tọa độ Y và tọa độ X.
Nén	Số nguyên từ 0 đến 99. “0” Không nén. “1” Được nén (xem phần 2).
Mã hóa	Số nguyên từ 0 đến 99. “0” Không mã hóa. “1”Được mã hóa.
Số cập nhật Base Cell	Đến khi một cell được tái bản thì số cập nhật hiện tại vào lúc tái bản sẽ được chèn vào đây. Nếu một phiên bản cell không được tái bản sau đó thì trường này được để trống hoặc có giá trị “0”.
Số cập nhật mới nhất của phiên bản trước đó	Để trống nếu không sẵn có phiên bản trước đó trong cơ sở dữ liệu của Data Server. Nếu phiên bản trước đó của cell sẵn có thì trường này sẽ chứa số cập nhật mới nhất của phiên bản trước đó.
Vị trí Base Cell (xem ghi chú ở dưới)	CD-ROMs. Vị trí trong Bộ sản phẩm trao đổi nơi Base Cell có thể được tìm thấy. Các Base Cell có thể được đặt trên một trong hai Bộ Sản phẩm trao đổi nền hoặc cập nhật. Đây là một số nguyên từ 1 đến 99 và bắt đầu bằng “B” nếu nó được lưu trên Base CD hoặc bằng “U” nếu nó được lưu trên Update CD. Ví dụ **B7, B11, U1,…** **Hỗ trợ Large Media** Trong trường hợp một dịch vụ hỗ trợ **Large Media,** trường

này được chia thành 2 trường con, tách biệt bởi dấu ";". Trường thứ nhất chứa số Media ID và trường thứ 2 chứa số Bộ sản phẩm trao đổi. Media ID được chỉ định là "M" theo sau là một con số. Số Bộ sản phẩm trao đổi được định dạng tương tự như trong CD-ROMs, ví dụ: **"B1"**. Ví dụ, một Cell cơ sở có thể được xác định vị trí theo cách sau: "M1;B1", "M1;B2", "M2;B10",… Ví dụ đối với Cell cập nhật: "M1;U1", "M1; U2" nếu nhiều hơn một Bộ sản phẩm trao đổi cập nhật trên cùng Media. Xem Phụ lục 2 của tài liệu này để biết thêm chi tiết.

Thay thế Cell bị xóa (Trường chú giải cũ)	Nếu một cell bị xóa và cell thay thế được phát hành thì trường này được sử dụng để nhận biết Cell thay thế. Trong trường hợp có nhiều hơn một Cell thay thế thì tên cell sẽ được tách biệt bởi dấu ";". Xem phần 6.2.3.3 để có thêm chi tiết.

LƯU Ý: "Base Cell Location" là vị trí đặt phiên bản mới nhất của Base Cell (cấu hình EN). Vị trí đặt này có thể trên CD gốc hoặc trong trường hợp có các Cell mới, các phiên bản hoặc dữ liệu tái bản mới thì đặt trên CD cập nhật.

Ví dụ về cấu trúc và định dạng của Product List ENC:




```
:DATE 20061213 09:22
:VERSION 1
:CONTENT FULL
:ENC
FR301130.000,20020316,2,20061124,2,21,50.0,-3.0,51.0,-2.0,,,,,,,,,,,,,,,,,,,,,1,1,0,2,B4,
FR301140.000,20061025,3,20061102,23,725,49.0,-3.0,50.0,-2.0,,,,,,,,,,,,,,,,,,,,,1,1,22,3,B4,FR312345;FR323456
FR301150.000,20030412,3,20061124,26,744,48.0,-3.0,49.0,-2.0,,,,,,,,,,,,,,,,,,,,,1,1,0,8,B4,
FR301160.000,20020413,2,20051206,13,87,49.0,-4.0,50.0,-3.0,,,,,,,,,,,,,,,,,,,,,1,1,0,5,B4,
FR301170.000,20020803,2,20061003,12,502,48.0,-4.0,49.0,-3.0,,,,,,,,,,,,,,,,,,,,,1,1,0,3,B4,
FR301180.000,20030830,3,20061114,1,34,49.0,-5.0,50.0,-4.0,,,,,,,,,,,,,,,,,,,,,1,1,0,3,B4,
```

6.2.3.1 Quản lý Cell bị xóa (Data Server)

Khi một Cell bị xóa bởi HO thì một tập tin Ceel cập nhật được tạo ra, chỉ chứabản ghi thông tin chung về Tập dữ liệu với trường "Data Set Identifier" [DSID]. Trường con "Số phiên bản" - "Edition Number" [EDTN] của trường DSID phải được thiết lập là "0". Thông báo xóa chỉ được sử dụng khi xóa một tập tin Base Cell.

Trong một dịch vụ được mã hóa, thông tin này không có sẵn cho Data Client trừ khi bản cập nhật được giải mã đầu tiên. Để tránh nhu cầu giải mã trước tiên có hai phương pháp mã hóa trong một Bộ sản phẩm trao đổi đã mã hóa như sau:

1. Trường con EDTN của trường CATD-COMT trong tập tin CATALOG.031 (xem mục 6.4.1.1).

2. Trường "Base Cell Edition" trong tập tin PRODUCTS.TXT (xem mục 6.2.3).

Tập tin CATALOG.031 có thể được sử dụng để nhận biết các cellbị xóa

trong Bộ sản phẩm trao đổi khi nhập vào trong tập tin PRODUCTS.TXT,để đánh dấu các cell bị xóa trong Dịch vụ của Data Server. Các ENC bị xóa còn lại trên Base CD hoặc Update CD ít nhất 12 tháng, bao gồm các tham khảo trong tập tin PRODUCTS.TXT.

6.2.3.2 Quản lý các Cell bị hủy bỏ (Data Client)

Các Cell ENC bị xóa này được loại bỏ khỏi Dịch vụ ENC của Data Server sẽ không còn được hỗ trợ hoặc được cập nhật bởi cơ quan được quyền phát hành. Có hai tùy chọn có sẵn cho nhà sản xuất khi quản lý các Cell bị xóa như sau:

1. Tự động loại bỏ Cell từ SENC khi một cell được biết là đã bị xóa.
2. Cho phép người dùng quyết định giữ lại hay là xóa bỏ cell trong SENC.

Các nhà sản xuất ECDIS/ECS tự quyết định các tùy chọn này để triển khai trong hệ thống của họ. Tuy nhiên, quan trọng là hệ thống thông báo cho người dùng việc các Cell cụ thể bị xóa và trong trường hợp tùy chọn 2 thì kết quả là giữ lại các cell.

Với tùy chọn 1, người dùng phải được thông báo để biết từng cell cụ thể bị xóa trong suốt thời gian tải hoặc tốt nhất là ghi báo cáo vào cuối quá trình xử lý.

Với tùy chọn 2, người dùng được chọn giữ lại hay loại bỏ cell từ SENC.Nếu người dùng chọn giữ lại Cell thì một tin nhắn cảnh báo thường xuyên được hiển thị trên màn hình, khi đó cell bị xóa sẽ được nhìn thấy. Thông báo tương tự ví dụ sau:

"Cell <name> has been cancelled and may not be up to date. Under no circumstances should it be used for primary navigation".

"Cell<tên> đã bị xóa và có thể lỗi thời.Không được sử dụng nó cho mục đích hàng hải".

6.2.3.3 Thay thế cell ENC bị xóa

Trong trường hợp một cell ENC bị xóa, nó thường được thay thế bằng một hoặc nhiều cell ENC khác. Điều này có thể do sắp xếp lại cho các Data Server. Sự cung cấp dữ liệu được thực hiện trong phiên bản này của S-63 để hiển thị thông tin này trên Data Client.Trường "Comment – chú giải" của tập tin PRODUCTS.TXT bây giờ có sẵn để hiển thị thông tin liên quan đến các Cell được thay thế.Định dạng bản ghi Cell trong danh sách sản phẩm được quy định trong phần 6.2.3.

Khi một cell được xác định là đã bị xóa, Data Client sẽ đọc trường "Cancelled Cell Replacement -Thay thế Cell bị xóa" để kiểm tra, nếu tại đó được thay thế bằng một cell ENC mã hóa. Nếu sau đó Data Client tạo sẵn thông tin này cho người dùng, một thông báo tương tự như sau sẽ được hiển thị:

"Cell <name> has been cancelled and has been replaced by cell(s), <name1>; <name2>. Please contact your data supplier to obtain the additional ENC permits".

"Cell <tên cell> đã bị xóa và được thay thế bởi cell khác <tên cell 1>; <tên cell 2>. Liên hệ với nhà phân phối dữ liệu của bạn để bổ sung thêm giấy phép ENC".

6.2.4 Phần Danh sách sản phẩm 'ESC'

Data Server có thể phát hành các loại sản phẩm bản đồ số khác như nền

tảng hải đồ, được sử dụng để hiển thị độ phủ hải đồ. Thông tin về các sản phẩm này cũng được tạo sẵn trong Danh sách sản phẩm nếu Data Server muốn.

Nội dung phần này giống với phần ENC được định nghĩa trong phần 6.2.3. Chỉ khác ở trường *"Section Identifier -Phần định danh"* sẽ là ":ECS".

Ví dụ mã hóa Danh sách sản phẩm sử dụng tất cả các đối tượng được định nghĩa trong phần 6.2.1.

```
:DATE 20061019 09:00:00
:VERSION 1
:CONTENT FULL
:ENC
AR201130.000,20051118,1,20060703,1,,-36.43335487,-57.41667361,-34.69998565,-
54.33335853,,,,,,,,,,,,,,,,,,,,1,1,0,0,B3,
AR302120.000,20051219,1,20060427,2,,-39.44997766,-62.39166614,-38.74168723,-
61.11683505,,,,,,,,,,,,,,,,,,,,1,1,0,0,B3,
AR402490.000,20051206,1,20060330,1,,-39.11668811,-61.94017540,-38.95167627,-
61.76656919,,,,,,,,,,,,,,,,,,,,1,1,0,0,B3,
AR402550.000,20051219,1,20060427,1,,-39.01664968,-62.16649373,-38.88332240,-
61.94017540,,,,,,,,,,,,,,,,,,,,1,1,0,0,B3,
AR402560.000,20051122,1,20060427,1,,-38.99166872,-62.39166614,-38.74168723,-
62.16649373,,,,,,,,,,,,,,,,,,,,1,1,0,0,B3,
AR420010.000,20060912,2,,,,-35.16832135,-56.07497834,-35.03499407,-
55.84166992,,,,,,,,,,,,,,,,,,,,1,1,0,3,B3,
:ECS
PM1WORLD.000,19990101,1,,,3000,-90,-180.0,90.0,180.0,-90.0,-
180.0,90.0,180.0,,,,,,,,,,,,,,,,,,0,0,,,B5,
```

6.3 Tập tin Serial (SERIAL.ENC)

Một tập tin tên là SERIAL.ENC được cung cấp sao cho Data Client có thể nhận biết các thông tin dưới đây trước khi nhập vào:

-IDcủa Data Server (đã đăng ký với SA)
- Tuần phát hành.
- Ngày phát hành.
- Loại CD (Base hoặc Update)
- Định dạng phiên bản
- Số Bộ sản phẩm trao đổi (trong một dãy Bộ sản phẩm trao đổi)

6.3.1 Định dạng tập tin SERIAL.ENC

Tập tin SERIAL.ENC được cung cấp để hỗ trợ hệ thống Data Client quản lý nhập ENC CDs được cung cấp bởi một Data Server cụ thể thông qua nhiều Bộ sản phẩm trao đổi.SERIAL.ENC nên là tập tin đầu tiên được đọc từ Bộ sản phẩm trao đổi khi nó chứa thông tin quan trọng về ID của Data Serverđược IHO ấn định, ngày xuất bản CD, loại CD, số CD trong Dịch vụ của Data Server cụ thể,…

Nội dung của tập tin này có thể tham chiếu chéo với các giấy phép đã cài đặt để kiểm tra tình trạng đăng ký mua của Data Client.

Trường ID	Vùng định nghĩa	Byte	Phạm vi	Lưu ý (Xem phía dưới)
Data Server ID	Ký tự	2	2 chữ-số bất kỳ	1

Trường ID	Vùng định nghĩa	Byte	Phạm vi	Lưu ý (Xem phía dưới)
Tuần phát hành	Ký tự	10	Ký tự ASCII bất kỳ	2
Ngày xuất bản	Ngày	8	YYYYMMDD	3
Loại CD	Ký tự	10	Base hoặc Update	4
Định dạng phiên bản	Số thập phân	5	01.00 – 99.99	5
Số Bộ sản phẩm trao đổi	Ký tự	6	B01-99X01-99 hoặc U01-99X01-99	6
Dấu phân tách cuối bản ghi	Số thập lục phân	3	0x0B0D0A	7

Lưu ý **Giải thích và mô tả**

1 Data Server ID nên được đăng ký với IHO; Khi Data Server cũng là HO thì mã cơ quan của tổ chức thu được từ S-62 – Mã cơ quan sản xuất được IHO công nhận.

2 Tuần phát hành định rõ tuần và năm mà CD được phân phối, ví dụ: **WK12-99, WK45-99, WK23-00,**…

3 Ngày xuất bản thông thường được định dạng kiểu ngày tháng năm,YYYYMMDD, ví dụ **19990414, 20000102, 20061102**,…

4 CD có thể được phát hành thành hai loại khác nhau:
BASE: định dạng sẽ được xác định là BASE, CD chứa tất cả các ENs và bất kỳ ERs thêm vào.
UPDATE: Định dạng sẽ được xác định là UPDATE, chứa bất kỳ ENs mới và tất cả ERs được phát hành từ khi phát hành đĩa Base CD mới nhất có liên quan.

5 Định dạng phiên bản mô tả phiên bản của tập tin SERIAL.ENC. Phiên bản liên quan đến phiên bản 1.1 của S-63 là **02.00.**

6 Trường này phải được sử dụng để cho thấy số Bộ sản phẩm trao đổi trong một dãy, ví dụ **B02X03,** tức là 2 Base CD trong tổng 3 Base CDs, **U01X01**tức là 1 Update CD trong tổng 1 Update CD.

7 Dấu phân cách cuối bản ghi gồm các ký tự nhị phân và vì vậy mối quan tâm nên lấy khi cố gắng chỉnh sửa tập tin- nó không được chỉnh sửa trong Windows Notepad. Đây là lý do tại sao tập tin SERIAL.ENC phải luôn được chỉnh sửa trong trình biên tập ASCII/Hex. Dấu phân cách thường không cần thay đổi. Dấu phân cách được sử dụng là **0x0B0D0A.**

Tập tin SERIAL.ENC sẽ được lưu trữ trực tiếp trong tập tin media gốc, ví dụ cùng cấp độ như thư mục ENC_ROOT và INFO.

Ví dụ về các Tập tin SERIAL.ENC

```
PRWK15-99   19990414BASE      02.00B02X030x0B0D0A

PRWK20-99   19990601UPDATE    02.00U01X010x0B0D0A
```

(ở đây, 0x0B0D0A là dấu phân tách kết thúc bản ghi được chuyển đổi thành Hex)

6.4 Tập tin Danh mục S-57 (CATALOG.031)

Trường "Data Set Identification" [DSID] được sử dụng bởi ECS/ECDIS để đảm bảo các tập tin Cell Base và CellUpdate được nhập vào SENC theo đúng trình tự và không bị bỏ sót. Từ lúc toàn bộ tập tin cell ENC được mã hóa, thông

tin trường DSID của mỗi cell là không có sẵn trong hệ thống OEM, trừ khi nó được giải mã đầu tiên.

Trường "Comments-chú giải" [CATD-COMT] trong mỗi bản ghi cell của tập tin CATALOG.031 được sử dụng để lưu trữ thông tin DSID được yêu cầu. Từ lúc tập tin CATALOG.031 làm cơ sở cho Bộ sản phẩm trao đổi và nhận biết vị trí các tập tin được lưu trữ phù hợp với ý tưởng của mục đích này.

Thông tin được lưu trữ trong trường này phảitương tự với thông tin được lưu trữ trong trường DSID của tập tin Cell, phù hợp với phần 5.7 của IHO S-57, Phụ lục A, Chi tiết kỹ thuật Sản phẩm. Điều này được tóm tắt trong bảng sau đây.Bảng này định rõ quy luật để mã hóa hồ sơ ứng dụng EN &ER của ENC.

Sự kiện	Đuôi mở rộng tập tin	EDTN	UPDN	UADT	ISDT	Chú giải
Cell ENC mới	.000	1	0	19950104	19950104	UADT< hoặc = ISDT
Update 1	.001	1	1	Bị cấm	19950121	Chỉ ISDT
Update 2	.002	1	2	Bị cấm	19950225	Chỉ ISDT
…						
Update 31	.031	1	31	Bị cấm	19950905	Chỉ ISDT
Tái bạn của 1 cell ENC	.000	1	32	19950905	19950910	UADT < hoặc = ISDT
Update 32	.032	1	32	Bị cấm	19951023	Chỉ ISDT
…						
Update 45	.045	1	45	Bị cấm	19951112	Chỉ ISDT
Phiên bản mới của cell ENC	.000	2	0	19951201	19951201	UADT < hoặc = ISDT
Update 1 cho phiên bản 2	.001	2	1	Bị cấm	19960429	Chỉ ISDT

Data Server phải trích xuất thông tin cần thiết từ trường DSID trước khi mã hóa và ghi thành mã trong trường CATD-COMT của tập tin CATALOG.031.Cấu trúc và định dạng của trường này được miêu tả chi tiết trong phần 6.4.1.Hệ thống Data Client phải đọc trường CATD-COMT để truy cập vào trường DSID trong một Bộ sản phẩm trao đổi không được mã hóa.

6.4.1 Cấu trúc và định dạng CATD-COMT

Thông tin DSID được lưu trữ trong trường CATD-COMT được chia nhỏ thành 4 hoặc 5 trường con tách biệt bởi dấu phẩy (,). Điều này phụ thuộc vào tập tin ENC có hồ sơ áp dụng EN hoặc ER. Cuối trường con được ngắt quãng bởi dấu chấm phẩy (;).

Ví dụ:

VERSION=1.0,EDTN=1,UPDN=0,UADT=20060703,ISDT=20060703;

VERSION=1.0,EDTN=1,UPDN=1,ISDT=20060710;

6.4.1.1 Mã hóa các cell bị xóa (xem phần 6.2.3, 6.2.3.1, 6.2.3.2, 6.2.3.3)

Từ một bản cập nhật được cung cấp chứa thông báo xóa bỏ, được xem như một ER. Do đó, mục đích của trường CATD-COMTnên được mã hóa như sau:

VERSION=1.0,EDTN=0,UPDN=2,ISDT=20060814;

Bảng sau minh họa điều kiện áp dụng cho tất cả loại giao dịch khác nhau:

Số phiên Bản	Số Ấn bản	Số cập nhật	Ngày áp dụng cập nhật UADT]	Ngày phát hành [ISDT]	Chú giải
VERSION =1.0	EDTN =1	UPDN =0	UADT=20060703	ISDT=20060703	Cell mới (EN)
VERSION =1.0	EDTN =1	UPDN =1	Bị cấm	ISDT=20060710	Cập nhật(ER)
VERSION =1.0	EDTN =1	UPDN =10	UADT=20060710	ISDT=20060717	Tái bản(EN)
VERSION =1.0	EDTN =1	UPDN =11	Bị cấm	ISDT=0060731	Cập nhật(ER)
VERSION =1.0	EDTN =2	UPDN =0	UADT=20060731	ISDT=0060724	Phiên bản mới(EN)
VERSION =1.0	EDTN =2	UPDN =1	Bị cấm	ISDT=0060807	Cập nhật(ER)
VERSION =1.0	EDTN =0	UPDN =2	Bị cấm	ISDT=0060814	Cell bị xóa (ER)

6.5 Quản lý ENC Update

Một tập tin được cung cấp cho phép Data Client kiểm tra tính tương thích và phù hợp của Bộ sản phẩm trao đổi ENC Updatecụ thể trước khi nhập vào. Data Client sử dụng tập tin này để kiểm tra Bộ sản phẩm trao đổi Base mới nhất được nhập vào hệ thống SENC phù hợp với bản cập nhật hiện tại đang được cài đặt trên ECDIS. Tập tin này miêu tả trạng thái hiện tại của tất cả Base CD liên quan tới một Dịch vụ của Data Server. Nó tên là STATUS.LST. Phần sau đây miêu tả chi tiết hơn về định dạng và nội dung.

6.5.1 Tập tin STATUS.LST

Tập tin này được lưu trữ trong thư mục INFO trên CD Update ExChange liên kết tới Base CD chỉ chứa một bộ CD hoặc nhiều bộ CD (xem Phụ lục 2). Nó được cung cấp sao cho Data Client có thể kiểm tra trạng thái hiện tại của SENC dựa trên Base CD có sẵn. Tập tin này được sử dụng để kiểm tra tính tương thích của một Bộ sản phẩm trao đổi Update với Base CD mới nhất cài đặt trên Data Server. Một Update CD PHẢI có sẵn đều đặn[10]trong Dịch vụ được cung cấp phù hợp với phiên bản này của tiêu chuẩn.

LƯU Ý: Khi Data Server phát hành một bản cập nhật mới, chỉ một Update CD sẽ được cung cấp. Tuy nhiên, có thể có nhiều hơn 1 Bộ sản phẩm trao đổi Update trên một Update CD đơn trong trường hợp các dịch vụ được cung cấp trên Large CD như DVD.

6.5.1.1 Định dạng tiêu đề Status

Tiêu đề là bản ghi có chiều dài cố định chứa các thông tin sau đây:

Trường ID	Định nghĩa	Byte	Phạm vi
ID của Data Server	Ký tự	2	2 ký tự chữ - số
Tuần phát hành	Ký tự	10	Ký tự ASCII
Loại Media	Ký tự	10	UPDATE
Ngày phát hành	Số thập phân	8	YYYYMMDD
Dấu phân cách cuối bản ghi	Số thập lục phân	2	CR/LF

Ví dụ về Tiêu đề Status:

GBWK15-08 UPDATE 20080403

6.5.1.2 Định dạng bản ghi Status

Trường ID	Định nghĩa	Byte	Phạm vi
Số Base CD	Ký tự	2-3	Chữ - số (ví dụ B1, B11, M2,…)
ID của Data Server	Ký tự	2	Chữ - số (ví dụ GB)

[10] Cho dù tất cả các Base được tái bản trong tuần giống nhau, mặc đù điều này được xem là không thể.

Tuần phát hành	Ký tự	7	Ký tự ASCII (WKWW-YY)
Thông tin người dùng	Ký tự	1-100	Chuỗi văn bản ASCII được chứa trong dấu ngoặc kép đơn (‘) [HEX 27] có thể được sử dụng như một nhắc nhở người dùng (xem lưu ý bên dưới)
Ngày phát hành Base CD	Số thập phân	8	YYYYMMDD
Dấu phân tách cuối bản ghi	Số thập lục phân	2	CR/LF

LƯU Ý: Thông tin này được sử dụng bởi Data Client như một thông báo tới người dùng. Đây là trách nhiệm của Data Server để đảm bảo “Thông tin người dùng” phù hợp với thông tin chứa trên nhãn Media (CD, DVD,…)

Ví dụ về Bản ghi Status:

B1,GB,WK52-07,’BASE CD 1 dated 27 December 2007’,20071227

M1,GB,WK19-07,’BASE MEDIA 1 dated 10 May 2007’,20070510

Hệ thống phải quản lý phù hợp để nhập dữ liệu cơ sở từ các Data Server khác nhau và lưu trữ thông tin cơ sở dữ liệu cài đặt. Khi tải lên một phương tiện lưu bản cập nhật mới (CD, DVD) Data Client sẽ kiểm tra Base CD mới nhất được liệt kê trong STATUS.LST có trùng lặptrên hệ thống. Nếu không hệ thống sẽ thông báo một tin nhắn tương tự như sau:

“This ‘Update Media’ is not compatible with the actual installed ‘Base Media’. Please install the following ‘Base Media’ first and then continue with the ‘Update Media’.”

<Field: User Information 1>

<Field: User Information 2>

<Field: User Information x> (where x is the base media number)

Tức là: Đĩa “Update Media” này không tương thích với “Base Media” hiện đang cài đặt. Vui lòng cài đặt “Base Media” thứ nhất và sau đó tiếp tục với “Update Media”.

<Trường: Thông tin người dùng 1>

< Trường: Thông tin người dùng 2>

< Trường: Thông tin người dùng x> (Với x là số Base CD)

Ví dụ:

“This ‘Update Media’ is not compatible with the actual installed ‘Base Media’. Please install the following ‘Base Media’ first and then continue with the ‘Update Media’.”

“BASE CD 2 dated 03 April 2008”

Tức là: Đĩa “Update Media” này không tương thích với “Base Media” hiện đang cài đặt. Vui lòng cài đặt “Base Media” thứ nhất và sau đó tiếp tục với “Update Media”.

‘BASE CD2 ngày 03/4/2008’

LƯU Ý: Người dùng chỉ được thông báo để cài đặt Base CD tương thích chứa các cell ENC được cấp phép.

Toàn bộ ví dụ[11]:

[11] Hầu hết các Data Server hiện nay phát hành tất cả Base CD của họ đồng thời công nhận rằng các Base CD này có thể chuyển sang một phương pháp tốt hơn để phát hành các Base CD.

Bản cập nhật liên kết với Base CD trong một Bộ sản phẩm trao đổi riêng, ví dụ CD:

```
GBWK15-08   UPDATE    20080403
B1,GB,WK52-07,'BASE CD 1 dated 27 December 2007',20071227
B2,GB,WK14-08,'BASE CD 2 dated 03 April 2008',20080427
B3,GB,WK07-08,'BASE CD 3 dated 08 February 2008',20080227
B4,GB,WK07-08,'BASE CD 4 dated 08 February 2008',20080227
```

Bản cập nhật liên kết với Base CD trong nhiều Bộ sản phẩm trao đổi riêng, ví dụ DVD:

```
GBWK37-07   UPDATE    20070913
M1,GB,WK19-07,'BASE MEDIA 1 dated 10 May 2007',20070510
M2,GB,WK23-07,'BASE MEDIA 2 dated 07 June 2007',20070607
```

6.6 Tập tin S-57 Readme (README.TXT)

Data Server hiện đang sử dụng tập README.TXT để mã hóa thông tin quan trọng liên quan tới Dịch vụ của họ. Thông tin này có thể bao gồm:

1. Thông tin Dịch vụ tổng hợp được cung cấp bởi Data Server.

2. Thông tin cụ thể được cung cấp bởi RENC và các nhà sản xuất ENC riêng rẽ liên quan tới dữ liệu ENC của họ.

3. Thông tin cảnh báo về dữ liệu ENC cụ thể, chẳng hạn như phạm vi chồng đè ENC hoặc các vấn đề được biết đến với cell cụ thể.

Mặc dù sự bao gồm tập tin README.TXT không được yêu cầu trong Chi tiết kỹ thuật sản phẩm S-57, nhưng nó là một nguồn thông tin quan trọng trong tất cả các dịch vụ thương mại ENC, đặc biệt là khi số lượng ENC ngày càng tăng từ nhiều quốc gia sản xuất khác nhau.

Với suy nghĩ này, người ta khuyếncáocác hệ thống Data Client nên hiển thị tập tin này theo yêu cầu. Từ khi tập tin này còn xa lạ với người dùng, nó sẽ hữu ích cho hệ thống Data Client hiển thị khi cài đặt dữ liệu ENC để gây sự chú ý của họ.

7 CẤU TRÚC TẬP TIN VÀ THƯ MỤC

7.1 Giới thiệu

Lược đồ không yêu cầu sử dụng một cấu trúc tập tin hoặc thưmục cụ thể. Tuy nhiên, vì toàn bộ tập tin dữ liệu ENC đã mã hóa rất khó duy trì một số liên kết tập tin quan trọng, ví dụ như tập tin .txt và tập tin hình ảnh (.tiff) với các các tập tin cell ENC liên quan (base hoặc update). Cấu trúc thư mục được thông qua bởi Data Server được đưa ra trong ví dụ ở phần 7.5.1.1. Cấu trúc này cho phép tập tin .txt và hình ảnh được quản lý antoàn bằng cách duy trì một mối quan hệ trực tiếp giữa chúng và tập tin dữ liệu ENC tương ứng.

7.2 Quản lý tập tin S-57

Cấu trúc thư mục không cố định và có thể khác nhau giữa các Data Server. Vị trí tất cả các tập tin S-57 trong Bộ sản phẩm trao đổi đã mã hóa được định nghĩa trong tập tin CATALOG.031. Vậy là, đường dẫn tới tất cả các tập tin trong Bộ sản phẩm trao đổi được xác định trong từng bản ghi tập tin.

7.3 Cấu trúc tập tin (FILE)

Cũng như Bộ sản phẩm trao đổi [ENC_ROOT], thư mục gốc chứa thư mục tên là 'INFO' chứa tập tin PRODUCTURE.TXT (xem phần 6.2), STATUS.LST (xem phần 6.5) và phần bổ sunghoặc phần phụ chưa được định nghĩa. Các tập tin được xác định bởi các Data Server riêng. Thư mục gốc chứa tập tin SERIAL.ENC (xem phần 6.3). Mỗi tập tin cell ENC trong Bộ sản phẩm trao đổi ENC_ROOT có một tập tin Chữ ký tương ứng (xem phần 5.3).

Data Server hiện tại cung cấp Chứng chỉ xác nhận (.CRT) với một Bộ sản phẩm trao đổi đã mã hóa S-63 đểhỗ trợtriểnkhai S-63 phiên bản 1.0. Tập tin Chứng chỉ này chứa trong thư mục gốc. Phiên bản 1.1 không cung cấp tập tin này với các Bộ sản phẩm trao đổi S-63.Các Data Server tiếp tục hỗ trợ tập tin này trong một thời gian giới hạn sau đó nó sẽ rút lui khỏi Dịch vụ của họ.

OEM lập trình cho hệ thống của họ tự động phát hiện một Bộ sản phẩm trao đổi hoặc một nhóm Bộ sản phẩm trao đổi bằng bất cứ cách nào.Tuy nhiên, nó không nên được mã hóa cứng vào hệ thống. Nếu một CD chứa một định dạng không mong đợi, hệ thống nên mặc định tới một đường phù hợp sao cho người dùng có thể xác định bằng tay vị trí của thư mục ENC_ROOT của một Bộ sản phẩm trao đổi được yêu cầu. Một Bộ sản phẩm trao đổi S-63 phải luôn luôn chứa một thư mục tên là ENC_ROOT có chứa một tập tin CATALOG.031 riêng và ít nhất một bộ dữ liệu.

7.4 Đặt tên thư mục và tập tin

Tất cả tập tin và thư mục phải được đặt tên theo quy ước trong Chi tiếtkỹ thuật Sản phẩm IHO S-57 và tài liệu này. Các tập tin và thư mục trong Bộ sản phẩm trao đổi phải được mã hóa S-63 ở dạng chữ hoa.

7.5 Exchange Set Media

Data Server cung cấp Bộ sản phẩm trao đổi tới Data Client bằng cách sử dụng một vài phương pháp khác nhau. Ví dụ:

1. CD-ROM
2. DVD (Large Media Support)
3. Dịch vụ trực tuyến.

7.5.1 CD-ROM

Bộ sản phẩm trao đổi đã mã hóa được cung cấp bằng phương pháp này sẽ được đưa theo khối ID phù hợp với Lược đồ Bảo vệ dữ liệu S-57, ví dụ V01X03, V01X02,…S-63 được cung cấp như một Bộ sản phẩm trao đổi đơn qua nhiều CD-ROM nhưng kinh nghiệm đạt được bởi Data Server cho thấy điều này là không thích hợp. Hiện nay, phương pháp này được thực hiện bởi Data Server để phát hành các Bộ sản phẩm trao đổi riêng qua nhiều CD.

7.5.1.1 Định nghĩa Folder

Mặc dù ví dụ dưới đây dựa trên Base CD, Update CD là tương tự nhau, chỉ khác là Update CD không nhất thiết phảigiữ lại tất cả dữ liệu cell Base. Tuy nhiên, Update CD phải chứa dữ liệu có sự nhất quán và tuần tự cho Base CD mà nó được áp dụng.

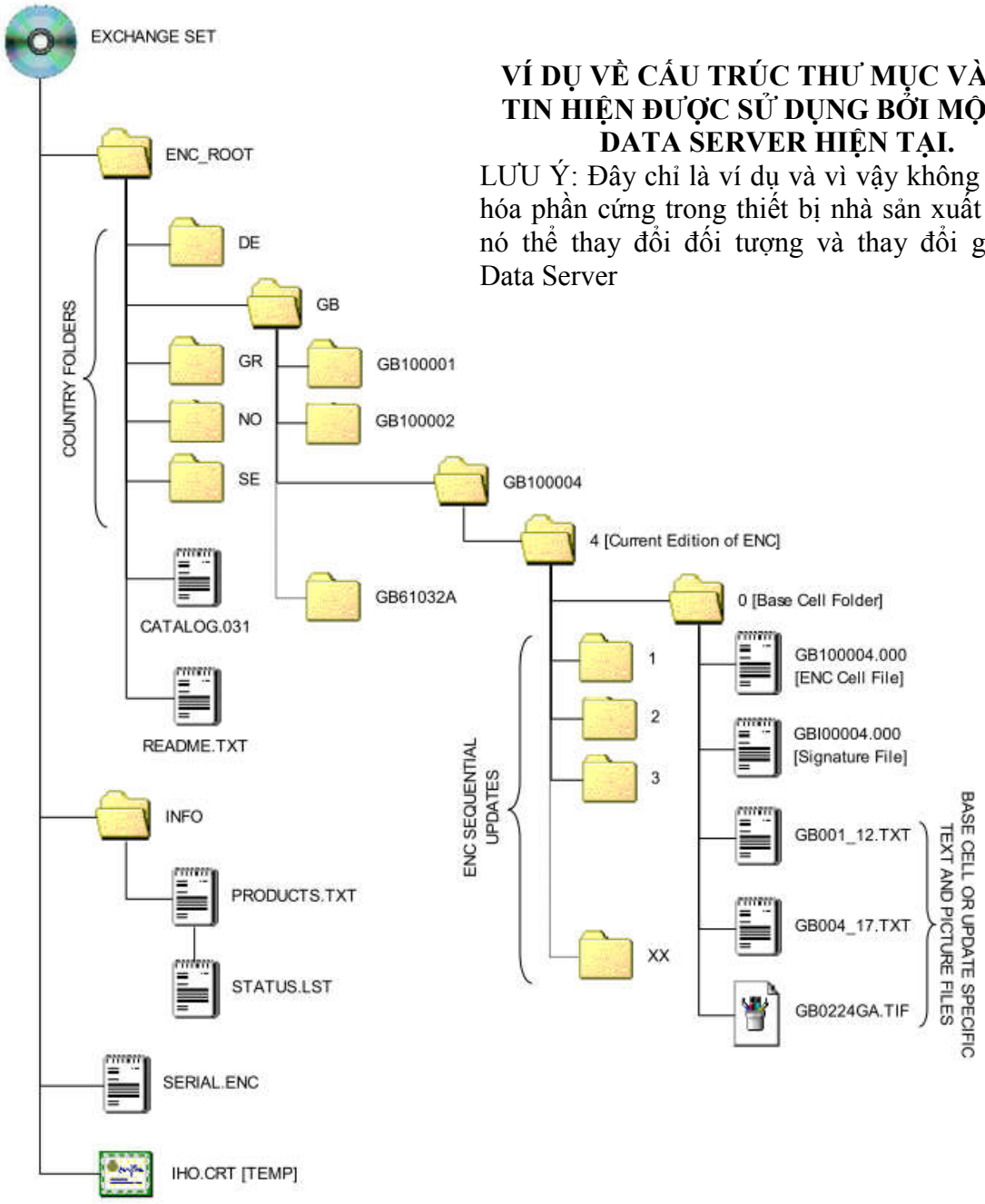
LƯU Ý: Vị trí tất cả các tập tin trong Bộ sản phẩm trao đổi [ENC_ROOT] có thể đọc từ tập tin CATALOG.031.

7.5.2 Large Media Support (DVD)

Large Media Support được định nghĩa là một thiết bị có khả năng lưu trữ khối lượng dữ liệu lớn hơnchuẩn CD-ROM. Chi tiết liên quan đến lưu trữ ENC mã hóa S-63 trên thiết bị được cung cấp trong Phụ lục 2.

7.5.3 Dịch vụ trực tuyến

Data Client có thể tải Bộ sản phẩm trao đổi từ RENC/VAR như được định nghĩa bởi nhà cung cấp dịch vụ.Tải về sau đó sao chép ra CD và tùy thuộc vào CD của RENC/VAR sẽ báo cho biết khối ID được ấn định cho CD. Điều này được lặp lại cho bất kỳ Bộ sản phẩm trao đổi được sao chép (ENC_ROOT), phải phù hợp với mục 5.4 của IHO S-57 Phụ lục B, Chi tiết kỹ thuật Sản phẩm.



VÍ DỤ VỀ CẤU TRÚC THƯ MỤC VÀ TẬP TIN HIỆN ĐƯỢC SỬ DỤNG BỞI MỘT SỐ DATA SERVER HIỆN TẠI.

LƯU Ý: Đây chỉ là ví dụ và vì vậy không nên mã hóa phần cứng trong thiết bị nhà sản xuất như nó nó thể thay đổi đối tượng và thay đổi giữa các Data Server

8 QUY TRÌNH QUẢN TRỊ LƯỢC ĐỒ

8.1 Nhà quản trị lược đồ bảo vệ dữ liệu.

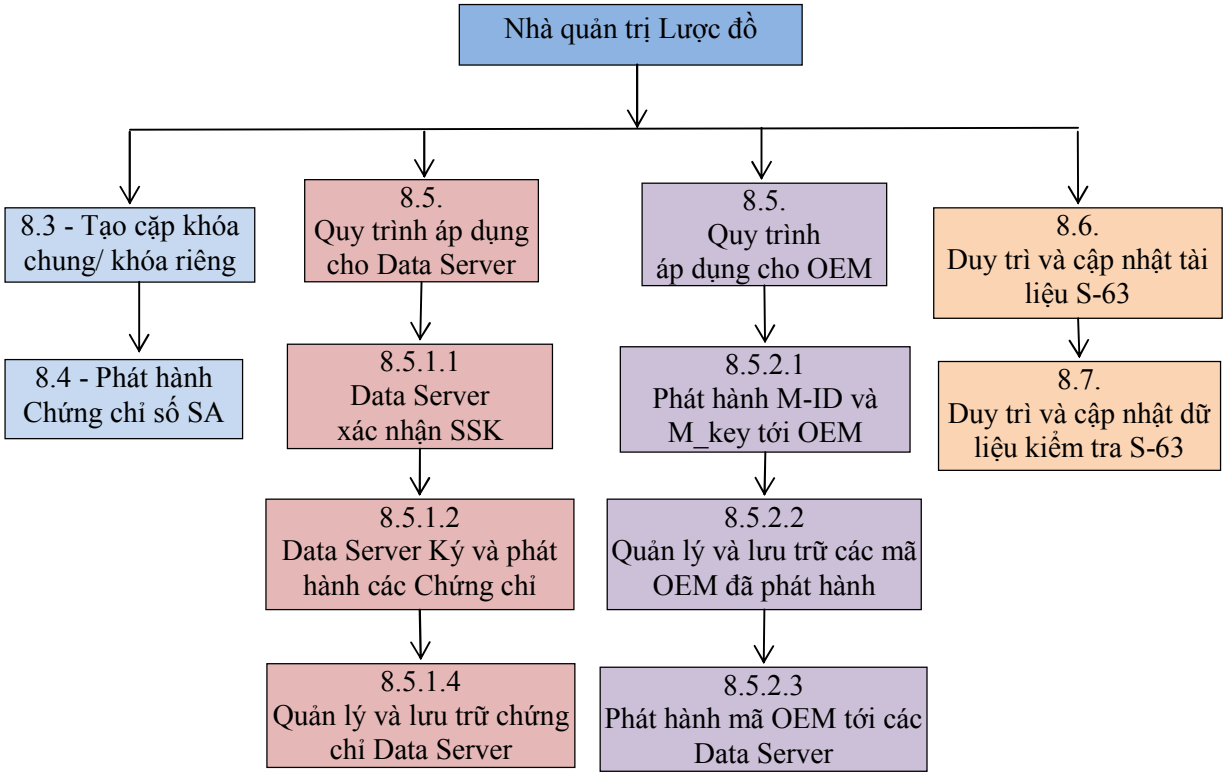
Nhà quản trị Lược đồ bảo vệ dữ liệu (SA) là duy nhất chịu trách nhiệm duy trì và phối hợp với Lược đồ Bảo mật dữ liệu hải đồ điện tử(S-63)(Data Protection Scheme-DPS). Vai trò của SA được vận hành bởi Cục Thủy đạc Quốc tế (IHB) như văn phòng của IHO, thay mặt cho các nước thành viên IHO.

SA chịu trách nhiệm kiểm soát hội viên của lược đồ và bảo đảm tất cả các bên tham gia vận hành theo đúng thủ tục đã được vạch ra. SA bảo quảncấp độ cao nhất các khóa mã hóa được sử dụng để vận hành toàn bộ lược đồ và là cơ quan duy nhất có thể phát hành chứng chỉ tới các bên tham gia khác.SA lưu giữ tất cả các tài liệu liên quan tới Lược đồ.

8.2 Quy trình quản trị lược đồ

Trách nhiệm chính của IHO cũng như Nhà quản trị lược đồ S-63 được

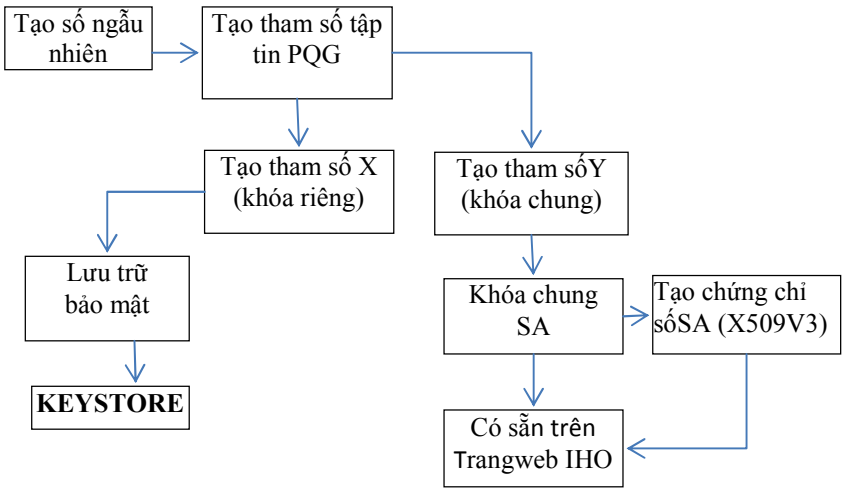
miêu tả trong sơ đồ bên dưới. Mỗi "Hộp quá trình" (ProcessBox)tham chiếu chéo đến một phần riêng biệt, nơi chứa các thao tác được tóm lược chi tiết hơn.



Quy trìnhquản trị lược đồ

8.3 Tạo cặp khóa mức cao nhất

IHO cũng như nhà quản trị lược đồ phải tạo cặp khóa chung và khóa riêngmức cao nhất. Khóa riêng sẽ được sử dụng để ký vào chứng chỉ Data Server và khóa chung để xác nhận chữ ký. Khóa chung phải được cài đặt trên hệ thống Data Client độc lập với dữ liệu ENC đã mã hóa.



Tạo cặp khóa mức cao nhất

8.3.1 Tạo tham số PQG

Thủ tục này thường được thực hiện bởi SA và Data Server trong lúc tạo cặp khóa chung/khóa riêng. Mặc dù các tham số PQG được tạo bởi Data Server không cần đồng nhất với tham số trong khóa chung SA và Chứng chỉ số SA, nhưng độ dài khóa sử dụng phải đồng nhất.

Tập tin PQG chỉ tự nó tồn tại trong một thời gian ngắn khi tạo các tập tin X và Y. Sau khi hoàn thành, tập tin PQG sẽ được chứatrong tập tin X và Y.

Việc tạo các tham số PQG thích hợp đượcchỉ dẫn chi tiết hơn trong ấn bản Tiêu chuẩn Chữ ký số (DDS-Digital Signature Standard) [2]. Thông tin liên quan đến định dạng của tập tin PQG xem phần 6.4.2.1.

8.3.2 Tạo khóa riêng

Khóa riêng là đầu ra của quá trình tạo khóa.Khóa riêng phải được lưu trữbảo mật và hạn chế truy cập và chỉ những người vận hành chương trình mới được phép biết.

Việcsở hữu trái phép khóa riêng của SA có khả năng phá hoạitính bảo mật trongphần xác thực của Lược đồ. SA sẽ phát hành một khóa chung mới (tương ứng với chứng chỉ SA) nếu khóa riêng bị xâm phạm. Định dạng tập tin X (khóa riêng) được miêu tả chi tiết trong phần 5.4.2.2.

8.3.3 Tạo khóa chung

Khóa chung là đầu ra của quá trình tạo khóa. Khóa chung được gửi đến các bên tham gia lược đồ cả dạng số và dạng in ra. Hai dạng này được gửi theohai phương pháp khác nhau. Định dạng tập tin Y (Public Key) được miêu tả chi tiết trong phần 5.4.2.3.

8.4 Tạo và phát hành Chứng chỉ số SA (X509v3)

Chứng chỉ số SA sẽ tuân theo X509v3 [4]. Chứng chỉ số SA sẽ luôn được cung cấp trong tập tin IHO.CRT. Tập tin IHO.CRT có sẵn trên trang web http://www.iho.int của IHO

SA sử dụng một khóa chung DSA dài 512 bit.

Tất cả Data Server cung cấp dịch vụ ENC có thể bao gồm chứng chỉ SA, để tham chiếu đến thư mục trên CD (ví dụ trong D:\IHO.CRT trên CD-ROM) như đã nêu trong phần 6.1, việc cài đặt chứng chỉ SA trên hệ thống Data Client nên thực hiện độc lập. Để kiểm tra tính hợp lệ của chữ ký SA trong tập tin chữ ký ENC phải thực hiện từ phiên bản cài đặt độc lập của chứng chỉ SA.

Khóa chung SA (trái với chứng chỉ số) có sẵn định dạng tập tin ASCII trên trang Webhttp://www.iho.int của IHO (định dạng được mô tả trong phần 6.5).

8.4.1 Cập nhật chứng chỉ số SA X509v3 (khóa chung)

SA sẽ tạo và công bố một chứng chỉ số SA mới trong các trường hợp sau:

- Khi Chứng chỉ số SA hết hiệu lực. Trong trường hợp này, chứng chỉ sẽ không chứa một khóa chung đã thay đổi.
- Khi khóa riêng SA bị xâm phạm. Trong trường hợp này, một khóa chung mới sẽ được chứa bên trong Chứng chỉ số SA.

SA sẽ công bố Chứng chỉ số mới của họ và nếu thích hợp, một phiên bản mới có thể được in ra (tham khảo phần 6.5) của khóa chung trên trang Web http://www.iho.int của IHO. Tất cả các Data Server và nhà sản xuất ngay lập tức được thông báo và sẽ nhận bản sao của Chứng chỉ số mới và nếu được áp dụng, khóa chung mới ở định dạng có thể in được.

Data Server và các nhà sản xuất chịu trách nhiệm thông báo cho Data Client của họ về Chứng chỉ số SA mới và nếu được áp dụng, thông báo thêm về khóa chung SA.

Thủ tục này thường được thực hiện bởi những người dùngLược đồ Bảo vệ

khi một Chứng chỉ số hoặc một khóa chung mới được phát hành và được thực hiện như sau:

- Thu về một Chứng chỉ số SA mới và một khóa chungdạng in ra được từ trang web http://www.iho.int của IHO.
- Ứng dụng sẽ tải một Chứng chỉ số SA mới và kiểm tra tính đồng nhất giữa khóa chung và khóa chung được in ra. Chỉ khi nào việckiểm tra tính đồng nhất hoàn thành thì ứng dụng mới cho rằng khóa chung SA là phù hợp. Tương tự như vậy, quy trình này được áp dụng để thay thế các khóa chung SA ban đầu.
- Thay thế Chứng chỉ số SA hiện cóbằngchứng chỉ mới phát hành.

8.5 Quy trình áp dụng cho Data Server và OEM.

Nhà quản trị lược đồ chịu trách nhiệm xử lý các đơn xin của Data Server và OEM muốn gia nhậpLược đồ Bảo mật dữ liệu hải đồ điện tử(S-63). Điều này bao gồm quản lý và phát hành Chứng chỉ được SA ký tới Data Server, quản lý và phát hành mã nhà sản xuất (M_ID và M_KEY) để OEM chấp thuận và phân phối tới Data Server được ủy quyền. Quá trình áp dụng được tóm lược chi tiết hơn tại **PHỤ LỤC A&PHỤ LỤC B** của tài liệu này.

8.5.1 Quy trình Data Server yêu cầu Chứng chỉ Data Server

Ứng viên Data Server sẽ được yêu cầu cung cấp một Chứng chỉ đã ký với khóa riêng của Data Server, gọi là Khóa tự ký (SSK-Seft Signed Key). Quy trình cấp chứng chỉ sau đó được thực hiện bởi SA và được miêu tả chi tiết ở phía dưới.

8.5.1.1 Xác thực tập tin Khóa tự ký (SSK)

SA xác thực tập tin SSK của Data Server trước khi tạo và phát hành một Chứng chỉ Data Server. Ban đầu, SA sẽ xác nhận SSK đó có được cung cấp ở định dạng phù hợp như miêu tả trong phần 5.4.2.5 hay không, nếu không phù hợp, quá trình sẽ kết thúc và một cảnh báo được đưa ra. Nếu phù hợp thì quá trình xác thực sẽ được tiếp tục như sau:

a) Trích xuất thành phần chữ ký ‘R’ và ‘S’ (tức là hai chuỗi dữ liệu đầu tiên và các tiêu đề đi kèm của chúng từ tập SSK được cung cấp bởi Data Server). Điều này để lại một tập tin khóa chung.

b) Băm tập tin khóa chung bằng cách sử dụng thuật toán SHA-1. Tất cả các byte trong tập tin này đều được băm.

c) Xác minh chữ ký (các thành phần loại bỏ ở mục ‘a’) bằng cách thông qua nó, cùng với tập tin khóa chung và băm của tập tin khóa chung (thu được tại mục b) bởi DSA. Kết quả xác minh sẽ trả về một trạng thái (phù hợp hoặc không phù hợp).

Nếu Chữ ký xác minh là đúng, SA có thể tạo Chứng chỉ Data Server.

8.5.1.2 Tạo Chứng chỉ Data Server

SA tạo chứng chỉ Data Server sau khi SSK được xác thực.Chi tiết về thuật toán chữ ký số DSA được bao gồm trong ấn phẩm Tiêu chuẩn Chữ ký số 186 FIPS (DSS). Thủ tục như sau:

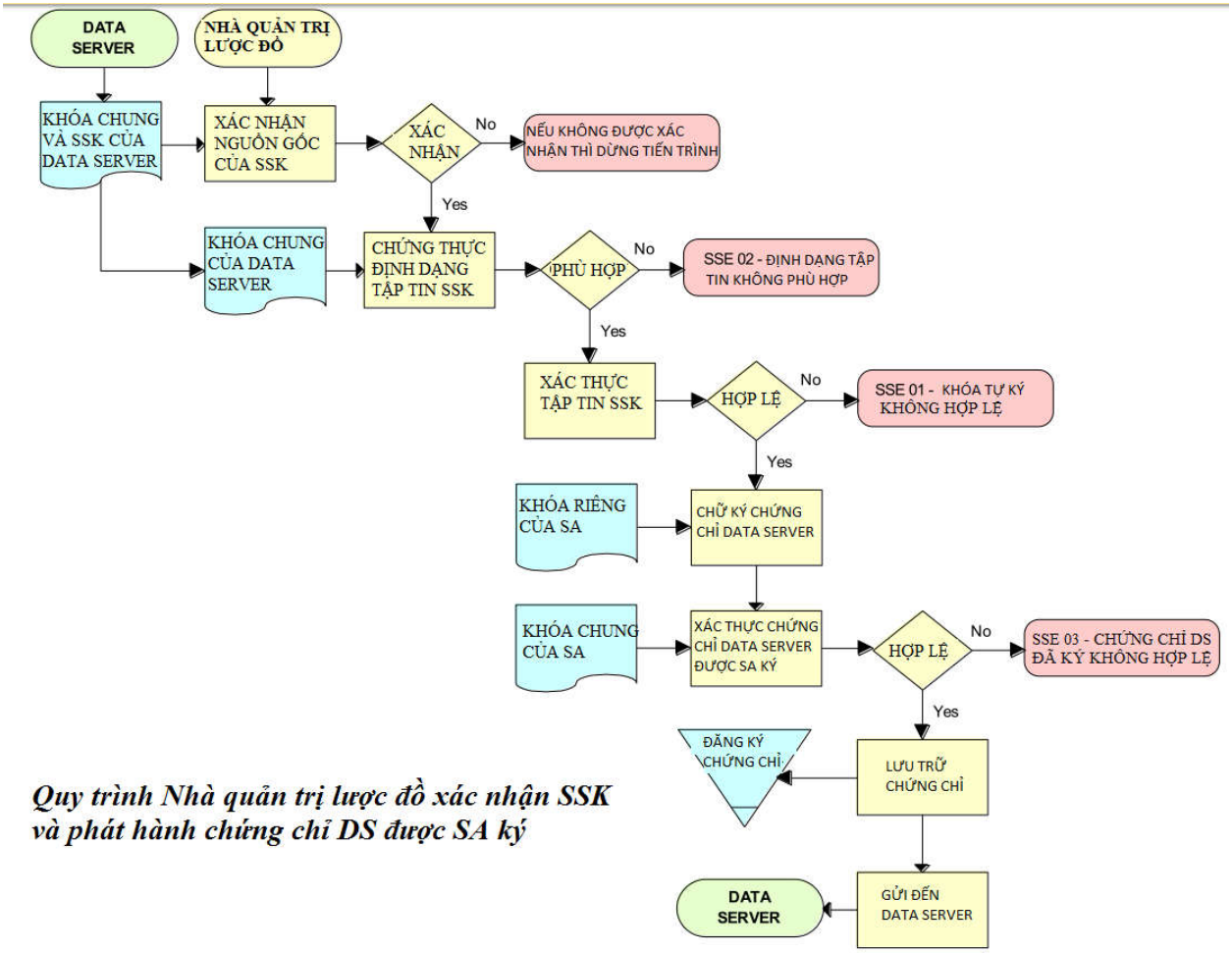
a) Loại bỏ các thành phần chữ ký (tức là hai chuỗi dữ liệu đầu tiên và các tiêu đề đi kèm) từ tập tin Khóa tự ký. Còn lại một tập tin khóa chung.

b) Băm tập tin khóa chung bằng cách sử dụng thuật toán SHA-1. Tất cả

các byte trong tập tin đều được băm.

c) Ký lên tập tin khóa chung (đã được băm tại mục b) bằng cách thông qua khóa riêng SA, băm của tập tin khóa chung (thu được ở mục b) và một chuỗi ngẫu nhiên của DSA. Việc này trả về 2 thành phần chữ ký (R và S).

d) Viết các thành phần chữ ký này lên tập tin Chứng chỉ và gán vào tập tin khóa chung (phần còn lại ở mục a) để tạo thành chứng chỉ.



Quy trình Nhà quản trị lược đồ xác nhận SSK và phát hành chứng chỉ DS được SA ký

8.5.1.3 SA xác nhận chứng chỉ Data Server được ký

SA xác nhận chứng chỉ mới được ký là hợp lệ trước khi gửi nó tới Data Server. Thủ tục như sau:

a) Trích xuất các thành phần chữ ký (tức là hai chuỗi dữ liệu đầu tiên và các tiêu đề đi kèm của chúng) từ tập tin Chứng chỉ Data Server mới được tạo. Điều này thu về tập tin khóa chung của Data Server.

b) Băm tập tin khóa chung Data Server (thu được từ mục a) bằng cách sử dụng thuật toán SHA-1. Tất cả các byte trong tập tin này đều được băm.

c) Xác minh các thành phần chữ ký (bị loại bỏ tại mục a) bằng cách thông qua nó, cùng với tập tin khóa chung SA và băm của tập tin khóa chung DS (thu được tại mục b) tới DSA. Điều này trả về một trạng thái (phù hợp hoặc không phù hợp).

Nếu Chứng chỉ Data Server được xác nhận là phù hợp, nó có thể được gửi

tới Data Server và được sử dụng trong cấu trúc của Chữ ký số ENC.

8.5.1.4 Quản lý Chứng chỉ Data Server

Khi một Chứng chỉ Data Server được SA ký đãphát hành tới Data Server nó được lưu trữ bảo mật trong một kho chứa chứng chỉ. Chứng chỉ được ấn định một Data Server duy nhất và tham chiếu chéo tới khóa riêng được sử dụng để ký vào nó và khóa chung được sử dụng để xác nhận phê chuẩn.

8.5.2 Quy trình OEM áp dụng

Nhà sản xuất (OEM) phải xin phép SA để trở thành thành viên của Lược đồ Bảo mật dữ liệu hải đồ điện tử(S-63).

8.5.2.1 Phát hành và quản lý mã nhà sản xuất theo S-63

Ứng viênOEM thành công được cung cấpmã ID nhà sản xuất (M_ID) và khóa nhà sản xuất (M_KEY) riêng của họ xem phần 4.2.4 và 4.2.5. Các mã này được lưu trữ an toàn cùng với thông tin các nhà sản xuất và dù họ có còn là một bên tham gia vận hành Lược đồ hay không.

8.5.2.2 Phát hành danh sách M_ID và M_KEY tới Data Server

Data Server yêu cầu giá trị M_ID và M_KEY để có thể nhận biết một nhà sản xuất cụ thể và thuvề M_KEY phù hợp để chiết xuất HW_ID của Data Client từ Userpermit. SA sẽ cung cấp cho Data Server một danh sách đầy đủ các mã nhà sản xuất đãđược phê duyệt theohệ thống S-63. Danh sách này sẽ được cung cấp một cách bảo mật mỗi khi một nhà sản xuất được thêm vào danh sách hoặc nếu trạngthái của nhà sản xuất thay đổi, ví dụ các thành viên rút khỏi lược đồ.

8.6 Dữ liệu thử nghiệm S-63

Lược đồ Bảo mật dữ liệu hải đồ điện tử(S-63) được hỗ trợ một bộ dữ liệu thử nghiệmtoàn diện - xem Phụ lục 1 S-63 – Dữ liệu thử nghiệm của Lược đồ Bảo mật dữ liệu hải đồ điện tử(S-63).

8.7 Nhà quản trị Lược đồ - Thủ tục bảo vệ QA

8.7.1 Tài liệu

SA nắm giữ tài liệu của Lược đồ Bảo vệ dữ liệu. Việc này được tổ chức theo thủ tục kiểm soát sự thay đổi và SA sẽ thông tin cho tất cả các bên tham gia (Data Server, nhà phát triển ứng dụng cho Data Client) Lược đồ bảo vệ dữ liệu, hoặc chuyển thành tiêu chuẩn.

Dữ liệu thử nghiệmcủa Lược đồ bảo vệ dữ liệu và cốt lõi phần mềm có sẵn cho hệ thống nhà sản xuất để kiểm tra sự triển khai có được tuân thủ đầy đủ.Dữ liệu dùng thử và cốt lõi phần mềm được miêu tả trong Phụ lục A, phụ lục B và trang web http://www.iho.int của IHO.

8.7.2 Quản lý Thỏa thuận bảo mật

Tất cả chi tiết cần thiết để vận hành Lược đồ bảo vệ và các thông tin độc quyền (ví dụ M_KEY) được cung cấp tới các bên có liên quan dưới dạngThỏa thuận bảo mật. SA chịu trách nhiệm quản lý các thỏa thuận này.Thỏa thuận bảo mật sẽ hạn chế khả năng các bên tham gia vi phạm Lược đồ bảo vệ dữ liệu.

8.7.3 Kiểm tra an ninhcác sổ đăng ký

SA có khả năng kiểm toán tất cả sổ đăng ký an ninh được duy trì giữa các bên tham gia Lược đồ Bảo vệ dữ liệu. Nội dung các sổ đăng ký này được định nghĩa trong mục 9.3.2.3, 9.3.3.3, 9.7.3 và 10.10.3. SA phải kiểm tra các sổ đăng ký này để xác nhận rằng chúng đã hoàn tất và được cập nhật. Nếu có vấn đề gì

phải được chỉnh sửa ngay lập tức hoặc các bên trở thành không tuân thủ và sẽ phải rút khỏi Lược đồ Bảo vệ.

8.7.4 Tạo M_ID và M__KEY

SA chịu trách nhiệm về việc tạo và phát hành giá trị M_ID và M_KEY được sử dụng trong Lược đồ bảo vệ dữ liệu.SA sẽ ghi lạitrong một sổ đăng ký M_ID/M_KEY tất cả các giá trị M_KEY/M_ID và các tổ chức nhận các giá trị này.SA đảm bảo rằng không có giá trị trùng với giá trị này được tạo ra.

SA sẽ cung cấp thông tin cho tất cả các Data Server trongLược đồ bảo vệ về việc sửa đổi giá trị M_ID và M_KEY.

8.7.5 Tạo khóa chữ ký số (khóa chung và khóa riêng)

SA có khả năng tạo một cặp khóa chung và khóa riêng. Khóa riêng được sử dụng trong quá trình ký vào chứng chỉ và khóa chungsử dụng trong quá trình xác nhận chữ ký.

Khóa riêng phải được lưu trữ bảo mật và hạn chế truy cập, chỉ những người vận hành chương trình mới được phép biết. SA sẽ phát hành một khóa chung mới (tương ứng với chứng chỉ SA) nếu khóa riêng hiện tại bị xâm phạm.

Khóa chung của SA được tạo sẵn cho tất cả các bên tham gia Lược đồ bảo vệ dữ liệu ở cả dạng số và dạng in ra, ví dụ như fax và tải về từ một trang web. Cả hai định dạng được gửi đi hoặc cung cấp theo2 phương pháp khác nhau.

8.7.6 Chấp thuận Khóa tự ký (SSK)

SA phải xác nhận rằng các Khóa tự ký được cung cấp bởi Data Server là hợp pháp bằng cách liên lạc với tổ chức ban đầu. Điều này có thể được thực hiện qua điện thoại, fax hoặc qua thư điện tử nhưng nguồn gốc phải được xác nhận để đáp ứng yêucầu của Nhà quản trị lược đồ trước khi Chứng chỉ DS được ký bởi SA bằng cách sử dụng Khóa tự ký. SA ghi lại các SSK nhận được vào sổ đăng ký SSK.

8.7.7 Tạo Chứng chỉ Data Server (DS)

SA có thể tạo Chứng chỉ DS được SA ký từ khóa tự ký được cung cấp bởi DS và khóa riêng của SA. Chứng chỉ đã ký sẽ được xác nhận dựa vào Khóa chung DS trước khi gửi tới DS. SA giữ một bản ghi tất cả các chứng chỉ DS trong một sổ đăng ký Chứng chỉ DS.

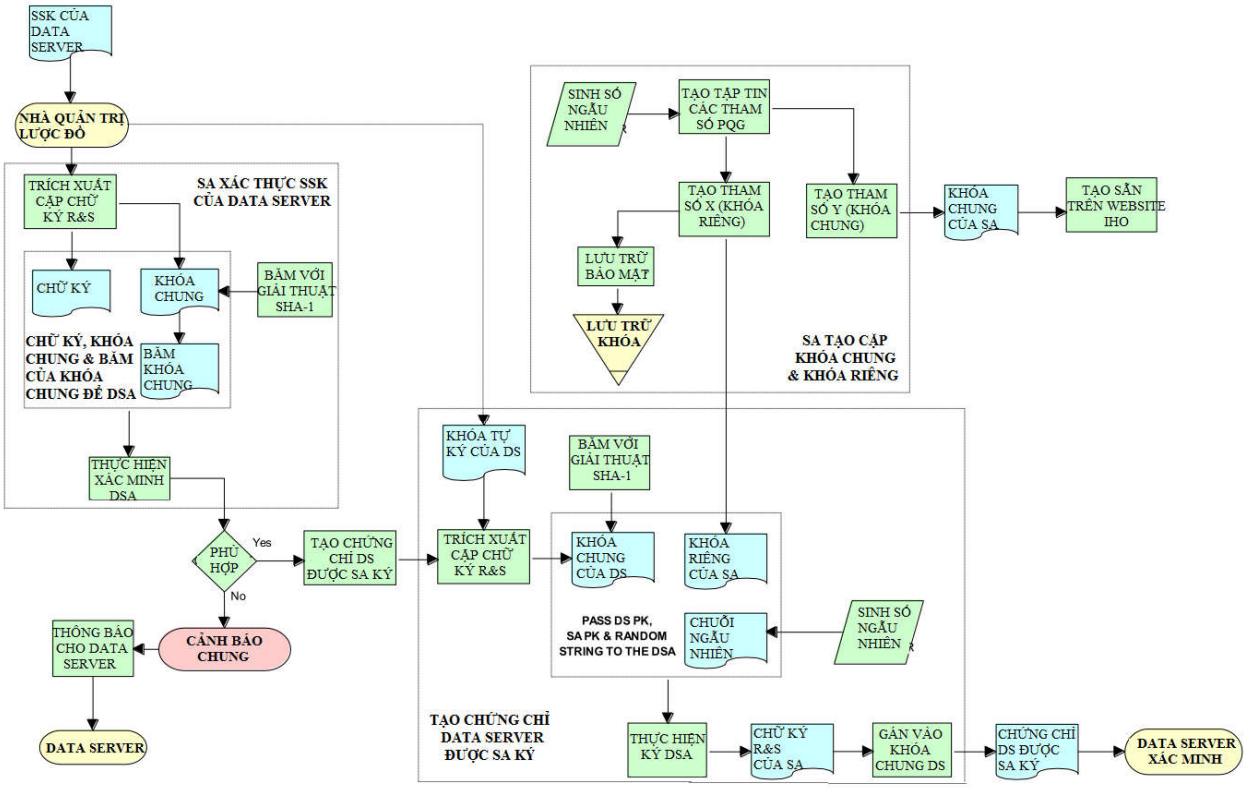
DS được yêu cầu ký vào một Thỏa thuận bảo mật trước khi SA phát hành Chứng chỉ DS. SA sẽ cung cấp thông tin tới tất cả các bên tham gia Lược đồ bảo vệ khi Chứng chỉ Data Server bị thu hồi.

8.7.8 Tạo các Chuỗi ngẫu nhiên

Để ký vào dữ liệu (được yêu cầu như một phần của việc tạo chứng chỉ), SA sẽ phải tạo một chuỗi ngẫu nhiên.SA đảm bảo rằng một giá trị giống nhau không được sử dụng cho 2 lần ký riêng biệt.Mặc dù SA không thể bảo đảm điều này nếu các chuỗi được tạo ra ngẫu nhiên.Tuy nhiên, xác suất để 1 chuỗi giống nhau được tạo ra 2 lần là vô cùng nhỏ.

8.7.9 Bàn giao M_ID và M_KEY

Khi hệ thống nhà sản xuất hoàn tất thử nghiệm tuân theo nội bộ của họ, họ sẽ yêu cầu ký một Thỏa thuận bảo mật trước khi SA phát hành M_ID và M_KEY.



Nhà quản trị lược đồ (SA) - Quy trình xác thự SSK và ký chứng chỉ

9 QUY TRÌNH CỦA DATA SERVER.

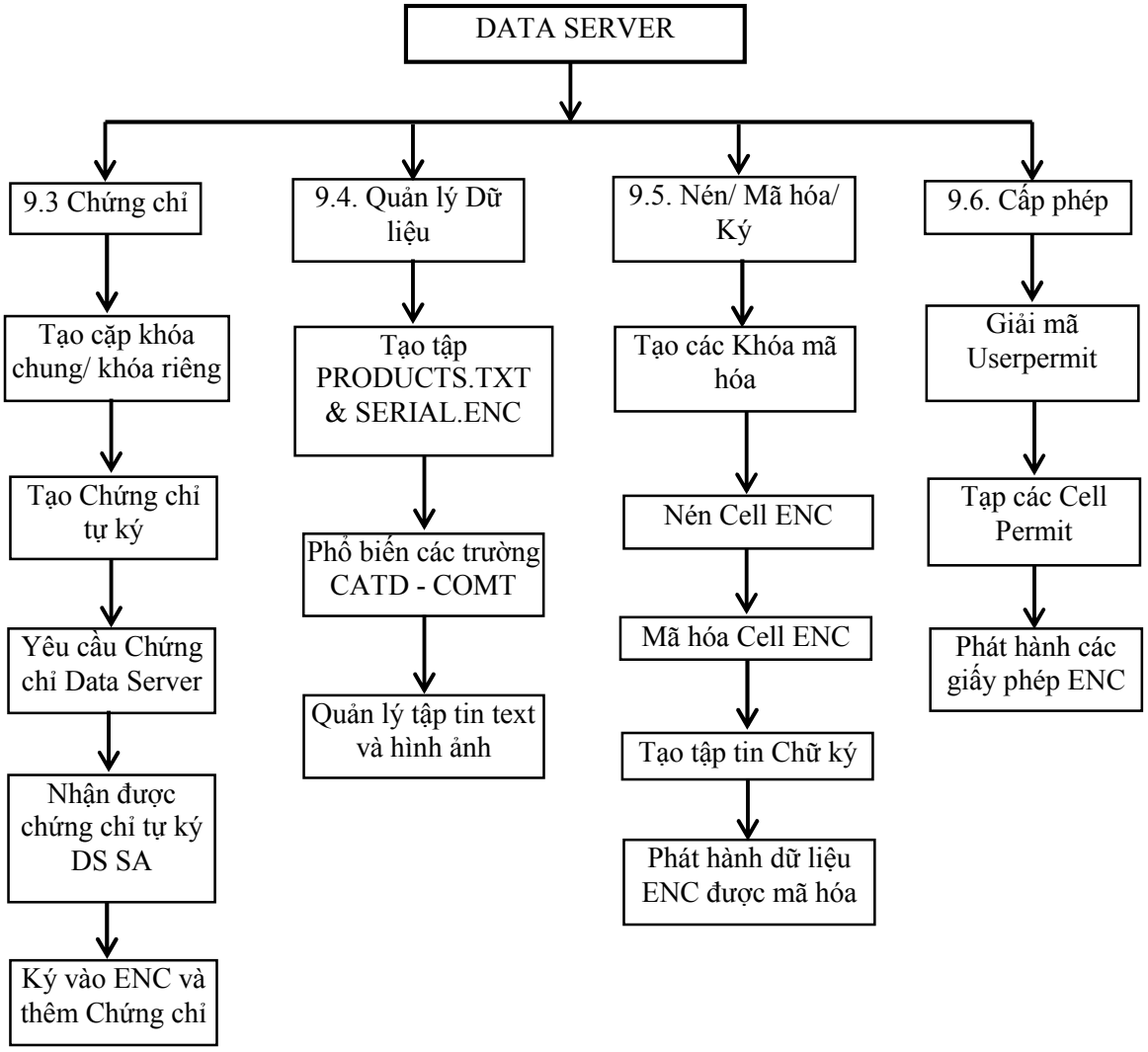
9.1 Khái quát chung

Data Server chịu trách nhiệm về mã hóa và ký vào thông tin ENC theo đúng thủ tục và phương pháp được định nghĩa bởi Lược đồ Bảo mật dữ liệu hải đồ điện tử(S-63).

Cơ quan Thủy đạc và tổ chức RENC là một trong các Data Server.Các tổ chức mong muốn trở thành Data Server đầu tiên phải ký tên và nộp một **Thỏa thuận Data Server S-63** cùng với một **Phiếu yêu cầu Chứng chỉ Data Server** hoàn chỉnh. Quy trình này được trình bày chi tiết trên trang web www.iho.int của IHO.

9.2 Quy trình của Data Server

Trách nhiệm chính của Data Server đã được phê duyệt hoạt động theo Lược đồ bảo vệ dữ liệu được miêu tả trong sơ đồ phía dưới.Mỗi mức độ trong "*Hộp xử lý- Process Box*" tham chiếu chéo đến một phần cụ thể mà các thao tác được tóm lược chi tiết hơn.


DATA SERVER
9.3 Chứng chỉ
Tạo cặp khóa chung/ khóa riêng
Tạo Chứng chỉ tự ký
Yêu cầu Chứng chỉ Data Server
Nhận được chứng chỉ tự ký DS SA
Ký vào ENC và thêm Chứng chỉ
9.4. Quản lý Dữ liệu
Tạo tập PRODUCTS.TXT & SERIAL.ENC
Phổ biến các trường CATD - COMT
Quản lý tập tin text và hình ảnh
9.5. Nén/ Mã hóa/ Ký
Tạo các Khóa mã hóa
Nén Cell ENC
Mã hóa Cell ENC
Tạo tập tin Chữ ký
Phát hành dữ liệu ENC được mã hóa
9.6. Cấp phép
Giải mã Userpermit
Tạp các Cell Permit
Phát hành các giấy phép ENC

9.3 Quy trình tạo chứng chỉ

9.3.1 Tạo cặp khóa chung/ khóa riêng.

Data Server cần tạo một cặp khóa chung và khóa riêng như một phần của phương pháp mã hóa "không đối xứng" được thực hiện bởi Lược đồ Bảo mật dữ liệu hải đồ điện tử(S-63). Khóa chung và khóa riêng của Data Server được sử dụng cho các nhiệm vụ sau:

- Khóa riêng được sử dụng để ký vào khóa chung của Data Server khi tạo Chứng chỉ tự ký (SSK).
- Khóa chung đượcsử dụng để chứng thực SSK trước khi nó được cung cấp tới SA.
- Khóa riêng được sử dụng để ký vào tất cả các tập dữ liệu ENC đã nén và mã hóa được tạo ra bởi Data Server.
- Khóa chung được sử dụng để kiểm tra tính toàn vẹn của tập tin dữ liệu ENC trong hệ thống ECS/ECDIS.

9.3.1.1 Tạo Bộ tham số chữ ký PQG

Thủ tục này thường được thực hiện bởi SA và Data Server trong quá trình tạo **cặp** khóa chung/khóa riêng. Mặc dù tham số PQG tạo bởi Data Server không cần giống tham số chứa trong khóa chung và chứng chỉ số của SA, nhưng chiều dài khóa được sử dụng phải giống nhau.

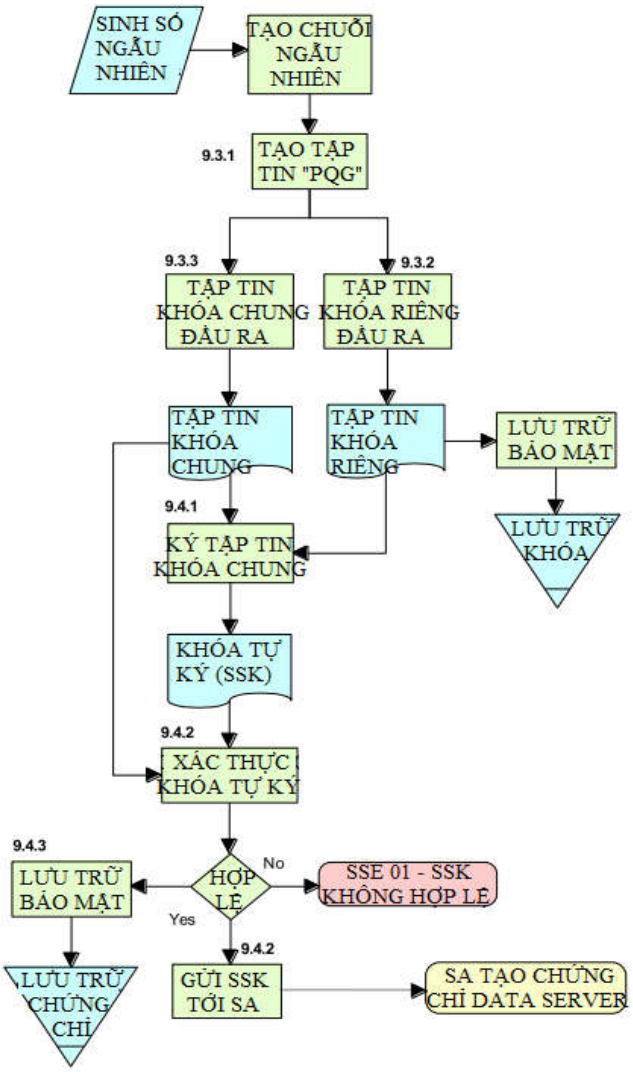
Tập tin PQG chỉ tồn tạitrong một thời gian ngắn khi tạo tập tin X và Y. Sau khi hoàn thành, tập tin PQG sẽ chứa trong tập tin X và Y.

Việc tạo các tham số PQG thích hợp được miêu tả chi tiết trong ấn bản Tiêu chuẩn Chữ ký số (DDS-Digital Signature Standard) [2].

9.3.1.2 Tạo tập tin khóa riêng

Khóa riêng là đầu ra của quá trình tạo PQG.Khóa riêng được lưu trữ bảo mật, chỉ những người vận hành chương trình mới được phép biết.

Việc sở hữu trái phép khóa riêng của SA có thể làm giảm tính bảo mật của phần xác thực của Lược đồ. SA sẽ phát hành một khóa chung mới (tương ứng với chứng chỉ SA) nếu khóa riêng bị xâm phạm. Chi tiết về định dạng tập tin X (khóa riêng) có trong phần 5.4.2.2.



Quy trình Data Server tạo cặp khóa chung/khóa riêng & Xác thực Khóa tự ký (SSK)

9.3.1.3 Tạo tập tin khóa chung

Khóa chung là đầu ra của quá trình sinh PQG. Khóa chung chứa trong Chứng chỉ Data Server được SA ký tạo thành một phần của tập tin Chữ ký ENC (xem phần 5.4.2.7). Hệ thống Data Client trích xuất thành phần khóa chung của tập tin này để kiểm tra tính toàn vẹn tập tin dữ liệu ENC dựa vào chữ ký ENC. Chi tiết về định dạng tập tin Y (Khóa chung) chứa trong phần 5.4.2.3.

9.3.2 Tạo Khóa tự ký của Data Server (SSK)

SSK được tạo ra và cung cấpcho SA để thu về một chứng chỉ Data Server. SSK chứa khóa chungcủa Data Server với một chữ ký được tạo bởi Data Server. Định dạng SSK giống với Chứng chỉ Data Server được định nghĩa trong phần 8.5.1.2, khác biệt duy nhất là SSK được tạo bởi Data Server và Chứng chỉ Data Server thì được tạo và phát hành bởi SA.

SSK xác định một chữ ký của khóa chung Data Server. Đầu vào cho chữ ký là khóa chung của Data Server, được định dạng theo định dạng tập tin khóa chung như miêu tả trong phần 5.4.2.3. Tập tin SSK phải viết dạng văn bản ASCII với định dạng, cấu trúc và thứ tự được miêu tả trong phần 5.4.2.5.

9.3.2.1 Đăng ký khóa chung và sinh khóa SSK

Thủ tục này thường được thực hiện một lần bởi Data Server để tạo Khóa tự ký của nó (SSK), sau đó được gửi tới SA, SA sử dụng nó để tạo chứng chỉ Data Server. Chi tiết về Thuật toán chữ ký số DSA được ghi rõ trong ấn bản Tiêu chuẩn chữ ký số FIPS 186 (DSS) [2]. Thủ tục như sau:

a) Băm tập tin khóa chungbằng cách sử dụng thuật toán SHA-1 [3]. Tất cả các byte trong tập tin đều được băm.
b) Đăng ký tập tin khóa chung (được băm ở mục "a" ở trên) bằng cách thông qua tập tin khóa riêng, băm của tập tin khóa chung (thu được tại mục "a" ở trên) và một chuỗi ngẫu nhiên thông qua thuật toán DSA [2]. Điều này trả về 2 thành phần chữ ký (R và S)
c) Viết các thành phần này vào tập tin khóa tự ký ở định dạng được xác định trong phần 5.4.2.5 và nối thêm vào tập tin khóa chung tạo thành tập tin khóa tự ký.

9.3.2.2 Xác nhận và phê chuẩn khóa SSK Data Server

Data Server phải xác thực SSK dựa vào khóa chung của Data Server để xác nhận rằng một SSK thích hợp đã được tạo ra.

a) Trích xuất thành phần chữ ký R và S (tức là hai chuỗi dữ liệu đầu tiên và tiêu đề kèm theo của chúng từ tập tin SSK được cung cấp bởi Data Server). Điều này để lại một tập tin khóa chung.
b) Băm tập tin khóa chung bằng cách sử dụng giải thuật SHA-1. Tất cả các byte trong tập tin đều được băm.
c) Xác minh chữ ký (các thành phần bị loại bỏ tại mục 'a' ở trên) bằng cách thông qua nó, cùng với tập tin khóa chung và băm của tập tin khóa chung (thu được từ mục 'b' ở trên) tới DSA. Điều này trả về một trạng thái hợp lệ hoặc không hợp lệ.

Nếu SSK là hợp lệ, sau đó nó có thể được cung cấp tới SA cùng với một bản sao khóa chungcủa Data Server.

9.3.2.3 Lưu trữ khóa tự ký

SSK được tạo ra bởi Data Server phải được lưu trữ bảo mật trong một Sổ đăng ký chứng chỉ và tham chiếu chéo tới cặp khóa chung/ khóa riêng liên quan.

9.3.3 Phê chuẩn các Chứng chỉ

9.3.3.1 Xác nhận Chứng chỉ số SA X509

Thủ tục này được thực hiện bằng cách:

a) Data Server là một phần để xác minh khóa chung SA được yêu cầu xác thực Chứng chỉ Data Server.
b) Data Client xác minh khóa chung của SA được sử dụng để xác thực chữ ký số cung cấp cùng với dữ liệu ENC.

Thủ tục của Data Server như sau:

So sánh thủ công khóa chung chứa trong Chứng chỉ số SA với một bản sao khóa chung in sẵn từ trang web http://www.iho.int của IHO. Nếu việc kiểm tra trên thất bại, Data Server sẽ không chấp nhận Chứng chỉ số SA.Ngược lại, Chứng chỉ số SA là hợp lệ và khóa chungSA có thể được sử dụng trong việc sản xuất tập tin chữ ký ENC.

9.3.3.2 Xác nhận Chứng chỉ Tự ký Data Server SA

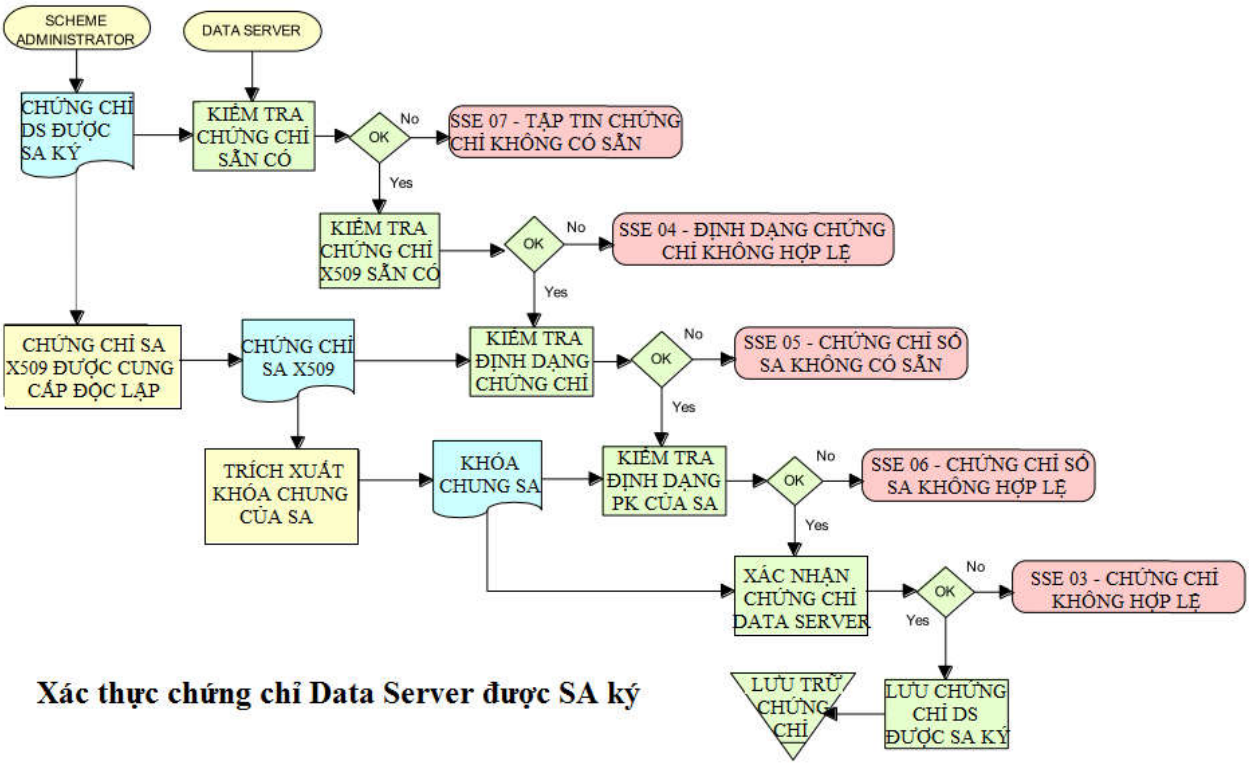
Thủ tục này thực hiện bởi Data Server để xác thực chứng chỉ thu từ SA trước khi nó được sử dụng. Nếu Data Server sử dụng một phương tiện tự động xác nhận thì sau đó phần mềm sẽ kiểm tra trước những thông tin sau sau:

a) Có sẵn một Chứng chỉ để xác nhận?.
b) Nếu có sẵn, thì cóở định dạng phù hợp phư phần 5.4.2.6.

Nếu sự thất bại được thông báo, trong hai tùy chọn quá trình này phải bị chấm dứt và một cảnh báo thích hợp được đưa ra.Ngược lại, quá trình xác thực sẽ xử lý như sau:

a) Thu về khóa chungSA từtrang web http://www.iho.int của IHO.
b) Trích xuất các thành phần chữ ký (tức là hai chuỗi dữ liệu đầu tiên và phần tiêu đề kèm theo của chúng) từ tập tin chứng chỉ. Kết quả thu được một tập tin khóa chung.
c) Băm tập tin khóa chung (thu được từ mục ‘b’) bằng cách sử dụng giải thuật SHA-1 [3]. Tất cả các byte trong tập tin đều được băm.
d) Xác minh thành phần chữ ký (bị loại bỏ tại mục ‘a’) bằng cách thông qua nó, cùng với khóa chung SA (khóa thu được tại mục ‘a’) và băm của tập tin khóa chung (thu được tại mục ‘b’) tới DSA [2]. Điều này sẽ trả về một trạng thái (phù hợp hoặc không phù hợp).

e) Nếu Chứng chỉ Data Server được xác nhận là đúng, các thành phần chữ ký R và S của nó có thể được sử dụng để xây dựng Chữ ký số ENC.



Xác thực chứng chỉ Data Server được SA ký

9.3.3.3 Lưu trữ chứng chỉ Data Server được SA ký

Tất cả các chứng chỉ được cung cấp bởi Nhà quản trị lược đồ phải được lưu trữ hết sức bảo mật trong Sổ đăng ký chứng chỉ và tham chiếu chéo với cặp khóa chung/khóa riêng và khóa SSK liên quan.

9.4 Quy trình quản lý dữ liệu

Quy trình quản lý dữ liệu bao gồm việc tạo và quản lý các tập tin để đưa vàotrong Bộ sản phẩm trao đổi đã mã hóa S-63, điều này bao gồm những phần sau:

a) Tập tin PRODUCTS.TXT (xem phần 6.2).
b) Tập tin SERIAL.ENC (xem phần 6.3)
c) Trường CATD-COMT của tập tin CATALOG.031 (xem phần 6.4.1)
d) Bản ghi tập tin văn bản và hình ảnh trong tập tin CATALOG.031 (xem phần 7.1).

Từng yêu cầu được quản lý cẩn thận trong sản phẩm phần mềm của Data Server và sẽ được tạo ra phù hợp với định dạng và quy ước miêu tả trong phần 6.

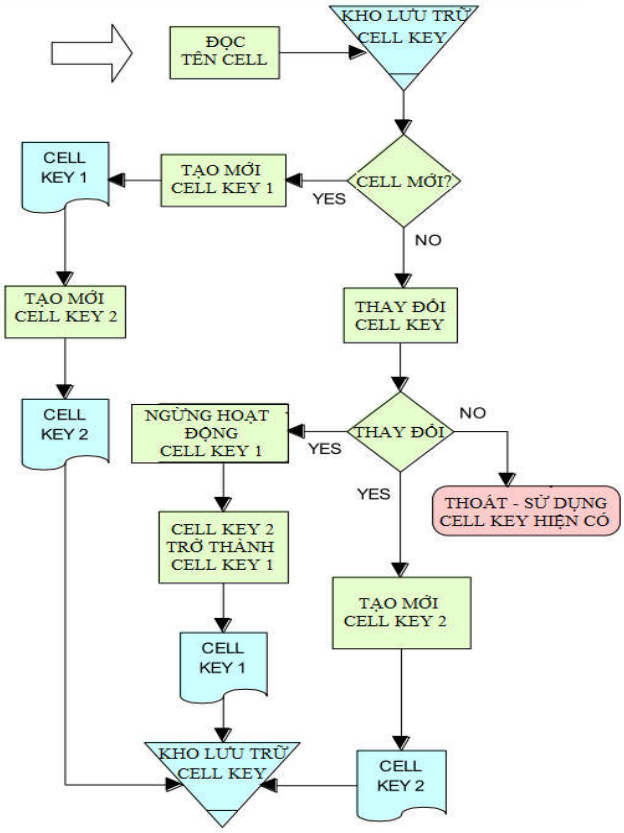
9.5 Quy trình mã hóa, nén và ký vào ENC.

9.5.1 Quản lý việc mã hóa Cell Key (ECK)

Mỗi ENC được mã hóa bằng cách sử dụng một Cell Key duy nhất và mỗi giấy phép ENC có khả năng lưu trữ hai Cell Key đã mã hóa. Các khóa này có thể tăng lên theo thời gian tùy thuộc vào ý muốn của Data Server vì vậy điều quan trọng là cần phải quản lý chúng một cách có hiệu lực và hiệu quả.

Để tạo Cell Key mới và tăng các Cell Key hiện có, Data Server yêu cầu một ứng dụng tự động quản lý các khóa và lưu trữ chúng một cách an toàn. Ứng dụng này phải có một phương thức sinh chuỗi ngẫu nhiên có độ dài chính xác và tốt nhất là có một phương tiện để đảm bảo rằngkhông được tạo ra các Cell Key trùng lặp trong một bộ.

Ứng dụng này phải có khả năng tạo các Cell Key mới cũng như quản lý việc tăng lên của các cell key đã có trong dịch vụ. Các bước sau đây cho thấy quy trình hợp lýkết hợp với quản lý khóa, lược đồ sau được sử dụng để minh họa thêm cho điều này.



Quy trình Data Server tạo và quản lý Cell Key

1. Lấy tên cell và nếu cần thiết lấy số phiên bản và xác định liệu nó có là một cell mới.
2. Nếu là cell mới thì tạo mới Cell Key 1 & 2, nếu không nhảy qua bước 4?
3. Lưu trữ cell key mới trong kho lưu trữ.
4. Nếu không phải là cell key mới, thì khóa có cần thay đổi không? Nếu không thì nhảy qua bước 5, nếu có thì nhảy qua bước 6.
5. Thoát và tiếp tục sử dụng cell key hiện có.
6. Cell key 1 bây giờ bị ngừng hoạt động và cell key 2 bây giờ trở thành cell key 1 và được đánh dấu như vậy trong kho lưu trữ.
7. Tạo Cell key 2 mới và thêm vào kho lưu trữ.

LƯU Ý: Việc tăng các cell key là theo ý muốn của Data Server trên cơ sở các quy tắc kinh doanh liên quan đến dịch vụ phân phối.

Ví dụ: các khóa có thể được tăng lên khi:

- Các khóa mã hóa hiện tại bị xâm phạm.
- Hàng năm hoặc khoảng thời gian được xác định bởi Data Server.
- Đồng bộ hóa với một phiên bản cell mới được phát hành.

9.5.1.1 Định dạng Cell key

Các cell key không được mã hóa dài 5 byte hoặc 10 byte ký tự thập lục phân (hex) như trong ví dụ phía dưới đây:

Cell Key 1	C1CB518E9C	5 bytes
Cell Key 2	421571CC66	5 bytes

9.5.2 Nén tập tin ENC (bản gốc hoặc bản cập nhật)

Thủ tục này thường được thực hiện bởi Data Server trên tập tin ENC trước khi chúng được mã hóa. Thủ tục này như sau:

- Nén tập tin cell ENC bằng cách sử dụng tiêu chuẩn ZIP [6], tài liệu tại

(www.pkware.com).

Kết quả nén tập tin ECN được sử dụng làm đầu vào cho giai đoạn mã hóa của Lược đồ.Chỉ tập tin cell ENC (gốc và cập nhật) là được nén. Quy trình này luôn hoàn thành trước khi dữ liệu được ký và mã hóa.

9.5.3 Mã hóa tập tin ENC

9.5.3.1 Tập tin ENC gốc

Thủ tục này được thực hiện bởi Data Server.Tập tin ENC phải được nén trước khi được mã hóa. Thủ tục này như sau:

a) Chọn **Cell Key** được sử dụng để mã hóa (xem điều kiện tại phần 9.5.1).
b) Mã hóa tập tin ENC bằng cách sử dụng giải thuật **Blowfish** với **cell key** (từ mục a) để tạo tập tin ENC đã mã hóa.

9.5.3.2 Tập tin ENC cập nhật

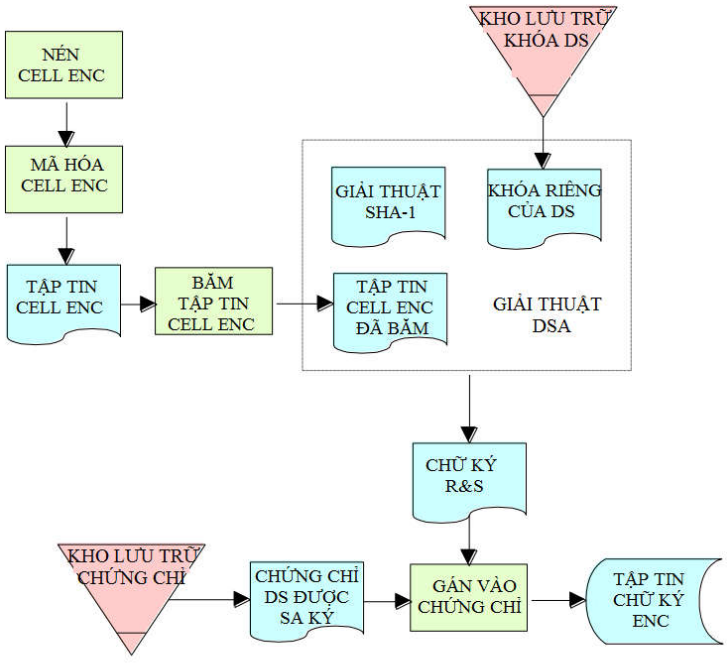
Thủ tục này được thực hiện bởi Data Server. Tập tin ENC cập nhật phải được nén trước khi được mã hóa. Thủ tục này như sau:

a) Lựa chọn **Khóa**được sử dụng để mã hóa tập tin ENC gốc mà bản cập nhật được áp dụng.
b) Mã hóa tập tin ENC cập nhật bằng cách sử dụng giải thuật **Blowfish** với **Khóa**(từ mục a) để tạo một ENC cập nhật đã mã hóa.

9.5.4 Ký vào tập tin ENC (bản gốc hoặcbản cập nhật)

Thủ tục này được thực hiện bởi Data Server để ký chữ ký số vào tập tin dữ liệu ENC của họ.Tập tin ENC phải được nén (phần 2 và 9.5.2) và được mã hóa (phần 6 và 9.5.3) trước khi chúng được ký. Thủ tục này như sau:

a) Thông qua khóa riêngcủa Data Server và nội dung tập tin ENC đã mã hóa với giải thuật DSA [2]. Giải thuật DSA sẽ băm tập tin ENC đã mã hóa bằng cách sử dụng giải thuật SHA-1 [3].
b) Giải thuật DSA trả về 2 tham số chữ ký cell (R và S)
c) Viết các các tham số này như hai chuỗi dữ liệu đầu tiên trong tập tin chữ ký phù hợp với định dạng và đặt tên theo quy ước quy định trong phần 5.4. Phần còn lại của tập tin được tạo thành từ Chứng chỉ Data Server chứa khóa chung kết hợp với khóa riêng được sử dụng để tạo Chữ ký.



Quy trình tạo tập tin chữ ký ENC

9.5.5 Phát hành dữ liệu ENC mã hóa S-63

Data Server sẽ phát hành Bộ sản phẩm trao đổi được mã hóa S-63 theo các nguyên tắckinh doanh phù hợp với dịch vụ cung cấp dữ liệu của họ.

9.6 Quy trình cấp giấy phép

9.6.1 Giải mã User Permit

Thủ tục này được thực hiện bởi Data Server để trích xuất HW_ID (mã nhận dạng hệ thống) nhằm tạo Cell Permit cho hệ thống Data Client.Cấu trúc User Permit được định nghĩa trong phần 4.2.1. Thủ tục để giải mã User Permit như sau:

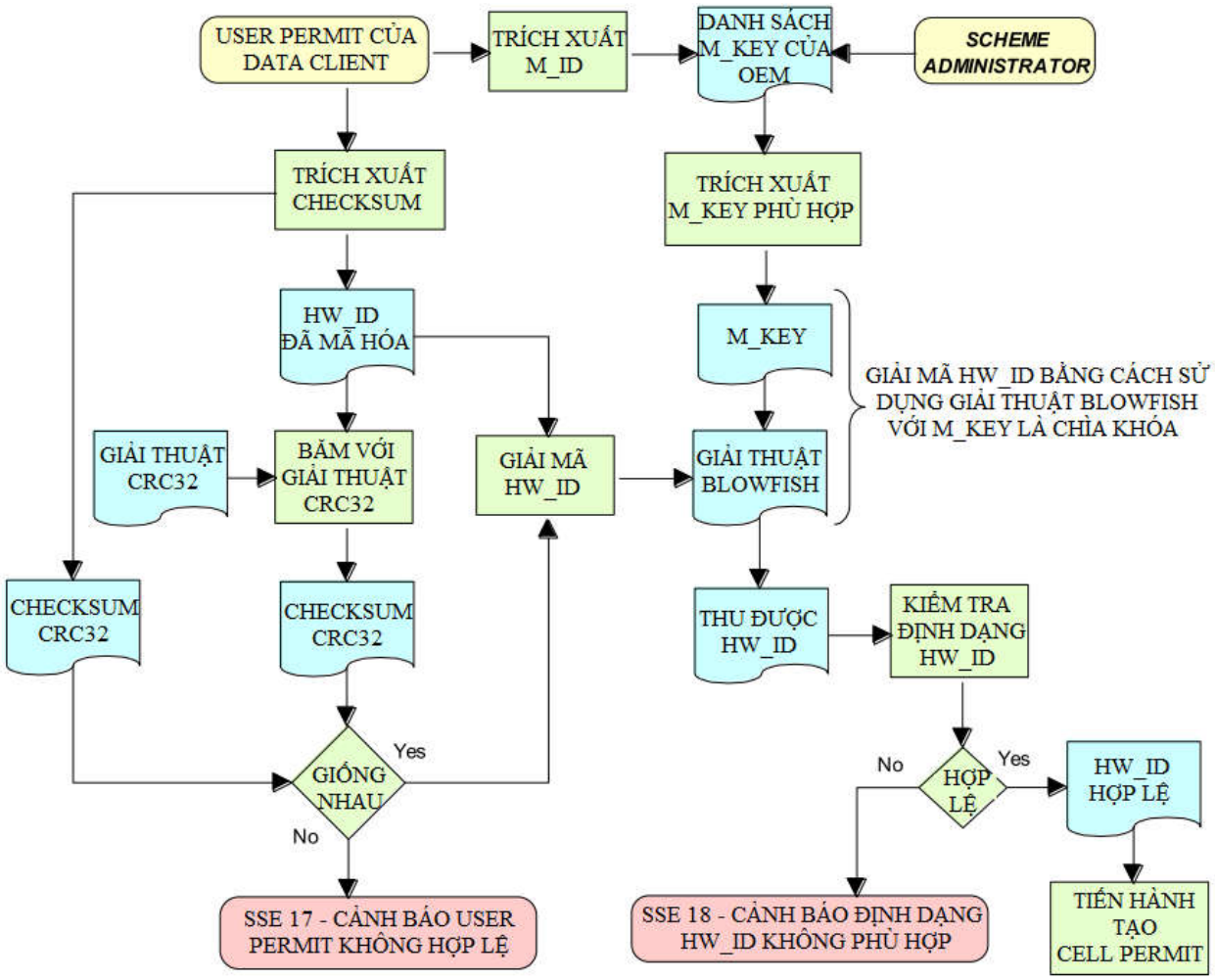
a) Trích xuất M_ID (4 ký tự Hex) từ User Permit.
b) Trích xuất Check Sum (8 ký tự Hex) từ User Permit.
c) Băm HW_ID đã mã hóa (16 ký tự đầu tiên của User Permit) bằng cách sử dụng thuật toán CRC32.
d) So sánh đầu ra ở mục 'b' và mục 'c'. Nếu chúng giống nhau thì User Permit là hợp lệ. Nếu khác nhau thì User Permit không hợp lệ và không thể thu vềHW_ID.
e) Nếu User Permit hợp lệ, chuyển đổi HW_ID đã mã hóa thành 8 byte.
f) Giải mã HW_ID đã mã hóa bằng cách sử dụng thuật toán **Blowfish** với M_KEY là chìa khóa. Đầu ra sẽ là HW_ID.

Data Server cần xác nhận rằng HW_ID nhận được có chiều dài phù hợp như định nghĩa trong phần 4.2.2.

Ví dụ:

User Permit	**73871727080876A07E450C043031**
M_KEY	**3938373635 (ASCII)**

Đầu ra từ mục 'a'		**3031**	M_ID được trích xuất
Đầu ra từ mục 'b'		**7E450C04**	Check Sum được trích xuất dạng Hex
Đầu vào mục 'c'		**73871727080876A0**	Các byte được trao cho hàm băm phía bên trái các byte đầu tiên (nghĩa là 73, sau đó 87, 17,…)
Đầu ra từ mục 'c'	**7E450C04**	Check Sum được trích xuất từ HW_ID đã mã hóa dạng Hex	
Đầu ra từ mục 'f'	**3132333438**	HW_ID dạng Hex	



Quy trình Data Server trích xuất HW_ID từ User Permit

9.6.2 Tạo Cell Permit

Quy trình để tạo Cell Permit được thực hiện bởi Data Server trên cơ sở yêu cầu của Data Client.Quy trình sau đây được sử dụng để tạo Cell Permit phù hợp với cấu trúc định nghĩa trong phần 4.3.

a) Loại bỏ phần mở rộng tập tin từ tên tập tin ENC. Còn lại 8 ký tự là tên cell của Cell Permit.
b) Gắn thêm ngày hết hạn giấy phép, ở định dạng YYYYMMDD vào têncell từ mục a.
c) Gắn byte thứ nhất của HW_ID vào phần cuối HW_ID để được HW_ID dạng 6 byte (gọi là HW_ID6). Điều này tạo một khóa 48 bít để mã hóa Cell Key.
d) Mã hóa Cell Key 1 bằng cách sử dụng thuật toán Blowfish với HW_ID6 từ mục ‘c’ là chìa khóa để tạo ECK1.
e) Chuyển đổi ECK1 thành 16 ký tự Hex. Các ký tự chữ cái đều dạng chữ in hoa.
f) Gắn vào ‘b’ đầu ra từ ‘e’.
g) Mã hóa Cell Key 2 (ECK2) bằng cách sử dụng thuật toán Blowfish với HW_ID là chìa khóa để tạo ECK2.
h) Chuyển đổi ECK2 thành 16 ký tự Hex. Các ký tự chữ cái đều dạng

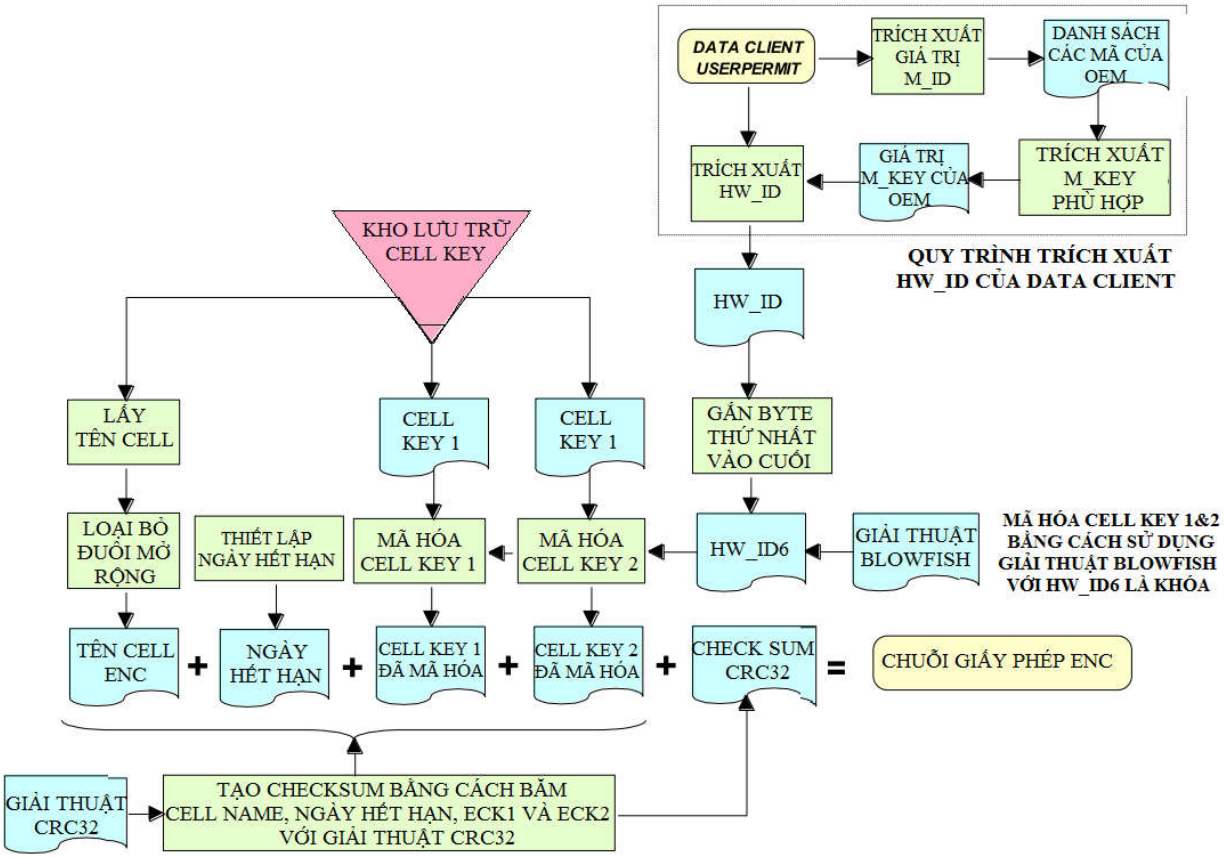
chữ hoa.

i) Gắn vào ‘f’ đầu ra từ ‘h’.
j) Băm đầu ra từ ‘i’ bằng cách sử dụng thuật toán CRC32. Lưu ý là băm được tính toán sau khi nó đã chuyển đổi thành một chuỗi hex trái ngược với User Permit nơi thuật toán băm được tính toán trên dữ liệu nhị phân chưa xử lý.
k) Mã hóa Băm (đầu ra từ ‘i’) bằng cách sử dụng thuật toán Blowfish với HW_ID là chìa khóa.
l) Chuyển đổi đầu ra từ ‘k’ thành chuỗi 16 ký tự Hex. Các ký tự chữ cái đều dạng chữ hoa. Đây chính là Check Sum của ENC.
m) Gắn vào ‘i’ đầu ra từ ‘l’. Đây chính là Cell Permit.

Ví dụ:

HW_ID	3132333438	5 byte dạng Hex
CK1	C1CB518E9C	5 byte dạng Hex
CK2	421571CC66	5 byte dạng Hex
Tên cell	NO4D0613.000	Tên cell phù hợp với S-57 bao gồm cả phần đuôi mở rộng
Ngày hết hạn	20000830	Định dạng YYYYMMDD

Đầu ra từ ‘a’	**NO4D0613**	Đây chính là tên cell
Đầu ra từ ‘b’	**NO4D061320000830**	Tên Cell + ngày hết hạn
Đầu ra từ ‘c’	**313233343831**	Đây là HW_ID6 dạng Hex
Đầu ra từ ‘d’ hoặc ‘e’	**BEB9BFE3C7C6CE68**	Đây là ECK1 dạng Hex
Đầu ra từ ‘f’	**NO4D061320000830BEB9BFE3 C7C6CE68**	Tên cell + ngày hết hạn +ECK1
Đầu ra từ ‘g’ hoặc ‘h’	**B16411FD09F96982**	Đây là ECK2 dạng Hex
Đầu ra từ ‘i’	**NO4D061320000830BEB9BFE3 C7C6CE68B16411FD09F96982**	Tên Cell + ngày hết hạn +ECK1 + ECK2
Đầu vào ‘j’	**NO4D061320000830BEB9BFE3 C7C6CE68B16411FD09F96982**	Các giá trị ASCII của đầu ra từ ‘i’ (toàn bộ 36 byte). Các byte được đưa cho hàm băm phía bên trái các byte đầu tiên (ví dụ xx, sau đó xx, xx,…)
Đầu ra từ ‘j’	**780699093**	CRC32 của ‘j’ số lượng 4 byte
Đầu ra từ ‘k’	**8 byte- không thể in ra.**	CRC32 được mã hóa
Đầu ra từ ‘l’	**795C77B204F54D48**	CRC32 được mã hóa dạng Hex
Cell Permit	**NO4D061320000830BEB9BFE3C7C6CE68B16411FD09F96982795C77B204F54D48**	



Quy trình Data Server tạo Cell Permit

9.6.3 Phát hành giấy phép ENC

Data Server phát hành giấy phép ENC để truy cập ENC đã mã hóa S-63 theođúng các nguyên tắc kinh doanh phù hợp với các dịch vụ phân phối dữ liệu của họ. Data Server sẽ tạo sẵn chi tiết về các dịch vụ của hocho Data Server trước khi các giấy phép được phát hành.

9.7 Thủ tục bảo mật QA – Data Server

9.7.1 Thông tin Lược đồ bảo vệ dữ liệu

SA cung cấp bản sao tất cả thông tin cần thiết để vận hành Lược đồ Bảo vệ dữ liệu đến một Data Server.

9.7.2 Kiểm tra sự tuân thủ hệ thống

Data Server phải thực hiện kiểm tra sự tuân thủ bên trong việc thi hành Lược đồ bảo vệ của họ, dựa trên miêu tả được cung cấp trong tài liệu này và dữ liệu dùng thử được cung cấp.

9.7.3 Lưu trữ M_ID và M_KEY

Khi Data Server tham gia lược đồ, SA sẽ cung cấp cho Data Server thông tin M_ID và M_KEY độc quyền của tất cả nhà sản xuất tham gia. SA ngay lập tức thông tin cho tất cả Data Server về sự sửa đổi danh sách M_ID và M_KEY khi có nhà sản xuất mới tham gia vào lược đồ.

Việc tiếp nhận tất cả M_ID và M_KEY bởi Data Server được ghi lại một cách bảo mật trong Sổ Đăng ký M_ID và M_KEY.

9.7.4 Kiểm tra và chấp nhận Chứng chỉ số SA (và khóa chung)

Data Server sẽ nhận được khóa chung của SA trong 2 định dạng, như là Chứng chỉ số X.509 và khóa chung có thể in được. Data Server có khả năng tải các Chứng chỉ số SA và tự so sánhcác khóa chungdựa vào khóa chung được in ra. Data Server chỉ chấp nhận khóa chung SA khi việc này được hoàn thành. Quá trình này được áp dụng cho khóa chung SA ban đầu và các khóa sau đóđược phát hành bởi SA.

Data Server sẽ lưu giữcác bản ghitrong **Sổ đăng ký khóa chung SA**; của những khóa chung SA đã được sử dụng. Những khóa chung này nên chứa trong một bản sao của mỗi khóa cũng như ngày mà nó được phát hành.

9.7.5 Tạo Khóa chữ ký số (khóa riêng và khóa chung)

Data Server có khả năng tạo một cặp khóa riêng và khóa chungcủa mình như được trình bày trong phần 9.3.

Khóa riêng phải được lưu trữbảo mật và hạn chế truy cập,chỉ những người vận hành chương trình mới được phép biết.Data Server tạo một cặp khóa chung/khóa riêng và yêu cầu một chứng chỉ Data Server từ SA nếu khóa riêng của nó bị xâm phạm.

Data Server sẽ tạo một Khóa tự ký (SSK) và gửi nó tới SA để chuyển đổi thành Chứng chỉ Data Server.Khi nhận được, SA sẽ liên hệ với Data Server gửi nó để xác nhận rằng SSK được cung cấp bắt nguồn từ nguồn đã đề ra.

9.7.6 Chấp nhận Chứng chỉ Data Server từ SA

Data Server sẽ xác minh và lưu trữ an toàn các Chứng chỉ được trả về bởi SA tuân theoquy trình được trìnhbày trong phần 9.3.3.3.

9.7.7 Tạo Cell Key

Data Server có khả năng tạo và quản lý Cell Key theo quy định trong phần 9.5.1. Data Server chịu trách nhiệm đảm bảo rằng các Cell Key được lưu trữ an toàn khi được tạo.

9.7.8 Nén, mã hóa và ký vào dữ liệu S-57

Data Server có khả năng nén, mã hóa và ký vào thông tin ENC theo quy định trong phần 9.5.2, 9.5.3 và 9.5.4. Truy cập tới chương trình ký nên bị hạn chế chỉ những có thẩm quyền phát hành dữ liệu mới được truy cập.

9.7.9 Tạo giá trị ngẫu nhiên

Để ký vào thông tin ENC, Data Server sẽ tạo các giá trị ngẫu nhiên. Data Server đảm bảo rằng không có giá trị giống nhau được sử dụng cho hai chữ ký riêng rẽ.

9.7.10 Tạo Cell Permit

Data Server phải có khả năng tạo Cell Permit cho Data Client. Data Server phải phát hành một Cell Permit mới tới Data Client của nó khi một cell ENC được mã hóa với một cell key khác (ví dụ: Khi phát hành một ấn bản mới).

9.7.11 Giải mã User Permit

Data Server phải có khả năng giải mã User Permit để thuvề HW_ID của Data Client. HW_ID được yêu cầu bởi Data Server để tạo một Cell Permit.

10 QUY TRÌNH CỦA OEM VÀ DATA CLIENT

10.1 Data Client

Data Client là người sử dụng thông tin ENC và nhận thông tin được bảo

vệ từ Data Server. OEM chịu trách nhiệm phát triển các ứng dụng phần mềm có khả năng xác nhận Chữ ký số ENC và mã hóa thông tin ENC tuân theo thủ tục được xác định trong Lược đồ Bảo vệ. Các nhà hàng hải với hệ thống ECDIS/ECS là ví dụ về Data Client.

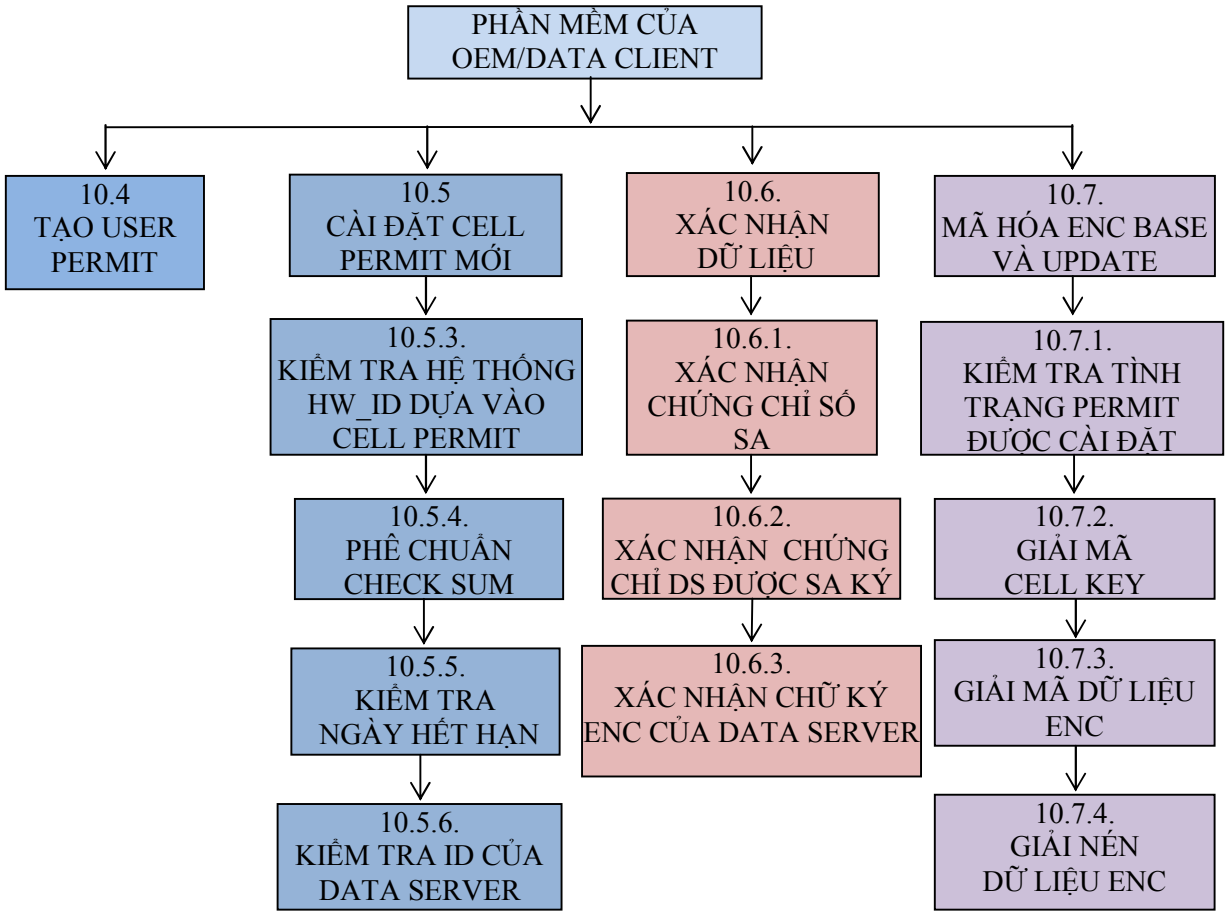
10.2 Nhà sản xuất thiết bị ECDIS/ECS (OEM)

Các nhà sản xuất đăng ký vào Lược đồ Bảo vệ dữ liệu phải xây dựng phần mềmtheo hỗ trợ của lược đồ.Tiêu chuẩn S-63 chứa chi tiết kỹ thuật và dữ liệu thử nghiệm để xác nhận ứng dụng phần mềm của nhà sản xuất.SA sẽ cung cấp cho nhà sản xuất một bộ mã nhà sản xuất duy nhất (M_ID và M_KEY).Nhà sản xuất cũng phải cung cấp cơ chế bảo mật bên trong hệ thống phần mềm của họ để xác định duy nhất một cài đặt người dùng cuối cùng.Lược đồ bảo vệ dữ liệu yêu cầu mỗi cài đặt có một mã nhận dạng phần cứng riêng (HW_ID). Data Server sẽ sử dụng thông tin M_KEY và M_ID để phát hành Cell Key ENC đã mã hóa tới một cài đặt cụ thể của Data Client. Mỗi ENC được mã hóa với một cell key riêng. Tuy nhiên, việc mã hóa dữ liệu bằng cách sử dụng mã HW_ID duy nhất của Data Client sẽ đảm bảo rằng chúng không bị chuyển giao giữa các ECDIS khác nhau được cung cấp bởi cùng một nhà sản xuất.

Nhà sản xuất được yêu cầu hợp tác để bảo vệ thông tin ENC trong hệ thống người dùng cuối cùng.Ví dụ, nếu một thiết bị phần cứng như một dongle (khóa cứng) được sử dụng để lưu trữ HW_ID, Data Client phải kiểm tra định kỳ sự hiện diện liên tục của nó.Data Client phải ngừng hoạt động nếu thiết bị bịgỡ bỏ sau khi ứng dụng được bắt đầu. Trên hệ thống mạng, thiết bị an ninh phải kiểm soát số lượng người đồng thời sử dụng ứng dụng; điều này phụ thuộc vào các điều khoản và điều kiện các dịch vụ Data Server.

10.3 Quy trình của OEM và Data Client

Trách nhiệm chính của OEM đã được phê chuẩn và các ứng dụng phần mềm của họ được miêu tả trong sơ đồ phía dưới. Mỗi "hộp xử lý-Process Box" tham chiếu chéo đến một phần cụ thể chứa các thao tác được miêu tả chi tiết.



Quy trình chính của Data Client/OEM

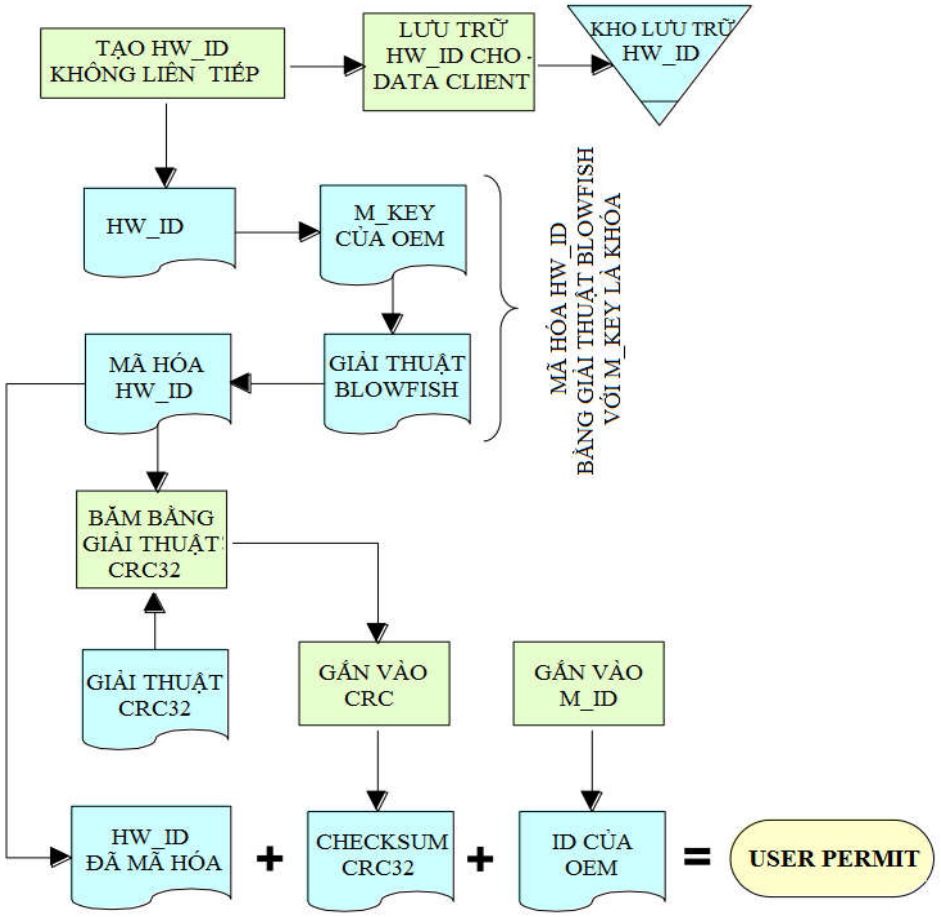
10.4 Tạo User Permit của Data Client

Thủ tục này được thực hiện bởi nhà sản xuất hệ thống (OEM) để tạo một User Permit riêng cho Data Client. User Permit được cung cấp cho Data Client khi mua hệ thống ECDIS/ECS. Userpermit này cho phép Data Client thuvề Cell Permit từ Data Server. Cell Permit được tạo ra bằng cách sử dụng HW_ID đã mã hóa chứa trong User Permit. Định dạng và cấu trúc của User Permit được định nghĩa trong phần 4.2.

Thủ tục để tạo User Permit như sau:

a) Mã hóa HW_ID bằng cách sử dụng thuật toán Blowfish với M_KEY là khóa.
b) Chuyển đổi giá trị kết quả thành một chuỗi 16 ký tự Hex. Các chữ cái ở dạng chữ hoa.
c) Băm 16 ký tự hex bằng cách sử dụng thuật toán CRC32.
d) Chuyển đổi đầu ra từ 'c' thành một chuỗi 8 ký tự Hex. Các ký tự chữ cái ở dạng chữ hoa. Đây là Check Sum.
e) Gắn vào 'b' đầu ra ở 'd'.

f) Chuyển đổi M_ID thành chuỗi 4 ký tự. Các chữ cái ở dạng chữ hoa.
g) Gắn vào ‘e’ đầu ra từ ‘f’. Đây chính là User Permit.



OEM - Tạo User Permit

Ví dụ:

HW_ID	**3132333438 (ASCII)**
M_KEY	**3938373635 (ASCII)**
M_ID	**3031 (ASCII)**

Kết quả dự kiến:

Đầu vào ‘a’	**3132333438** và **3938373635**	HW_ID và M_KEY dạng hex
Đầu ra từ ‘a’	**8** byte	Dạng không in được
Đầu vào ‘c’	**73871727080876A0**	Giá trị dạng hex của chuỗi trên. Các byte được đưa ra nhờ chức năm băm các byte bêntrái cùng (vd: 73, sau đó 87, sau đó 17,…)
Đầu ra từ ‘c’	**7E450C04**	Kết quả CEC32 dạng hex
Đầu ra từ ‘e’	**73871727080876A07E450C04**	Kết quả CRC32 được gắn vào HW_ID đã mã hóa
Đầu ra từ ‘f’	**3031**	Kết quả được gắnvào HW_ID và CRC_32 đã mã hóa
User Permit	**73871727080876A07E450C04 3031**	

10.5 Cài đặt Cell Permit ENC

Cell Permit mới được chuyển đến hệ thống Data Client trong một tập tin có tên PERMIT.TXT. Cấu trúc và định dạng của tập tin này được đưa ra trong phần 4.3.Hệ thống Data Client phải có khả năng đọc tập tin này và thực hiện việc kiểm tra. Mỗi bản ghi Cell Permit chứa một ID của Data Server cho phép OEM quản lý các giấy phép và dữ liệu trong trường hợp có nhiềunhà phân phối. Phần sau đây phác họa làm thế nào để quản lý và kiểm tra các tập tin này khi cài đặt một giấy phép mới.

10.5.1 Kểm tra Cell Permit

Hệ thống Data Client trước hết phải kiểm tra Cell Permit hợp lệ có sẵn khi cài đặt.Một tiện ích của Data Client để duyệtđến 1 vị trí cụ thể trên hệ thống khi tập tin PERMIT.TXTcó sẵn để cài đặt. Nếu có tập tin text khác tập tin có tên PERMIT.TXT được chọn, hệ thống sẽ trả về một cảnh báo như sau:

"SSE 11 - Cell permit not found" – "Không tìm thấy Cell Permit"

10.5.2 Kiểm tra định dạng Cell Permit

Nếu một PERMIT.TXT hợp lệ có trong hệ thống, thì phải kiểm tra rằng định dạng của tập tin này là đúng với định nghĩa trong phần 4.3. Nếu không thì Data Client phải thông báo cho người dùng như sau:

"SSE 12 - Cell permit format is incorrect" – "SSE 12 – Định dạng Cell Permit không chính xác".

~~10.5.3 Kiểm tra HW_ID~~

~~Hệ thống Data Client phải kiểm tra rằng HW_ID đã mã hóa trong dongle/thiết bị phần mềm bảo mật có thể so sánh với HW_ID đã mã hóa trong Cell Permit. Nếu giá trị là giống nhau, hệ thống sẽ tiếp tục kiểm tra như bên dưới. Ngược lại, một tin nhắn báo lỗi sẽ được trả về như sau:~~

~~**"SSE 19 - Permits are not valid for this system. Contact your data supplier to obtain the correct permits".**~~*("SSE 19 - Giấy phép không hợp lệ cho hệ thống này.Liên hệ với nhà phân phối dữ liệu của bạn để thu về giấy phép mới".)*

10.5.4 Kiểm tra Check Sum của Cell Permit

Thủ tục này được thực hiện bởi hệ thống Data Client, bao gồm các bước sau:

a) Trích xuất 16 ký tự hex cuối cùng (ENC Check Sum) từ Cell Permit.
b) Chuyển đổi 16 ký tự hex này thành 8 byte.
c) Băm phần còn lại của Cell Permit tại 'a' bằng cách sử dụng thuật toán CRC32.
d) Gắn byte đầu tiên của HW_ID vào cuối HW_ID để được dạng HW_ID 6 byte (gọi là HW_ID6).
e) Mã hóa file băm (đầu ra từ 'c') bằng cách sử dụng thuật toán Blowfish với HW_ID6 như là khóa.
f) So sánh đầu ra từ 'e' với đầu ra từ 'b'. Nếu chúng giống nhau, Cell Permit là hợp lệ, nếu chúng khác nhau thì Cell Permit không hợp lệ và không được sử dụng.

Ví dụ:

HW_ID	**3132333438**	Dạng Hex
Cell Permit	**NO4D061320000830BEB9BFE3C7C6CE68 B16411FD09F96982795C77B204F54D48**	Ví dụ Cell Permit

Đầu ra từ 'a'	**795C77B204F54D48**	Dạng Hex
Đầu ra từ 'b'	8 byte – không thể in được	Mã hóa CRC32
Đầu vào 'c'	**NO4D061320000830BEB9BFE3 C7C6CE68B16411FD09F96982**	Cell Permit sau khi loại bỏ 16 ký tự hex mã hóa CRC32. Các Byte được đưa tới hàmBăm các byte phía bên trái cùng (ví dụ xx, sau đó xx, sau đó xx,…)
Đầu ra từ 'c`'	780699093	4 byte CRC32 của Cell Permit sau khi loại bỏ 16 ký tự hex mã hóa CRC32
Đầu ra từ 'd'	313233343831	Đây là HW_ID6
Đầu ra từ 'e'	8 byte không thể được in ra	Mã hóa CRC32

Nếu giá trị CRC32 được tính toán không giống với giá trị chứa trong Cell Permit, hệ thống phải thông báo cho Data Client như sau:

"SSE 13 - Cell Permit is invalid (checksum is incorrect) or the Cell Permit is for a different system". – *["SSE 13 - Cell Permit không hợp lệ (Check Sum không chính xác) hoặc Cell Permit được dùng trên một hệ thống khác"].*

Hệ thống phải không cài đặt bất kỳ Cell Permit không hợp lệ.

10.5.5 Kiểm tra ngày hết hạn Cell Permit.

Khi cài đặt một tập tin PERMIT.TXT mới, hệ thống Data Client phải kiểm tra rằng các giấy phép được cài đặt chưa hết hạn. Hệ thống phải kiểm trangày hết hạn của mỗi giấy phép dựa vào ngày hệ thống (Computer Clock) và nếu có sẵn thời gian từ thu nhận/tín hiệu GPS. Nếu giấy phép đã hết hạn, một thông báo như sau được hiển thị:

"SSE 15 - Subscription service has expired. Please contact your data supplier to renew the subscription licence."- *"SSE 15- Đã hết hạn sử dụng giấy phép.Vui lòng liên hệ nhà phân phối dữ liệu của bạn để làm mới giấy phép sử dụng".*

LƯU Ý:Hệ thống có thể cài đặt giấy phép đã quá hạn/giấy phép hợp lệ nhưng bất cứ cell nào sau đó được hiển thị cho người xem theo các điều kiện này **PHẢI** hiển thị một cảnh báo thường xuyên cho người dùng như sau:

"SSE 25 - The ENC Permit for this cell has expired. This cell may be out of date and MUST NOT be used for NAVIGATION." – *"Giấy phép cho ENC đã hết hạn.Cell này có thể đã lỗi thời và KHÔNG ĐƯỢC sử dụng cho HÀNG HẢI".*

Xem phần 10.7.1.1 để kiểm tra ngày hết hạn tại thời điểm tải.

Nếu ngày hết hạn của giấy phép là trước giờđồng hồ máy tính/tín hiệu GPS, sau đó buộc phải kiểm tra thêm trong bao lâu thì giấy phép còn hiệu lực. Nếu là 30 ngày hoặc ít hơn 30 ngày thì hệ thống đưa ra một cảnh báo tới Data Client như sau:

"SSE 20 - Subscription service will expire in less than 30 days. Please

contact your data supplier to renew the subscription licence."–*"Dịch vụ đăng ký sẽ hết hạn trong vòng chưa đầy 30 ngày.Vui lòng liên hệ tới nhà cung cấp dữ liệu của bạn để gia hạn giấy phép đăng ký".*

Data Client có thể thực hiện từng bước để làm mới giấy phép trước khi nó hết hạn.Hệ thống sau đó sẽ tiếp tục cài đặt các giấy phép.Nếu các giấy phép có nhiều hơn 30 ngày trước khi hết hạn thì giấy phép sẽ được cài đặt mà không có cảnh báo.

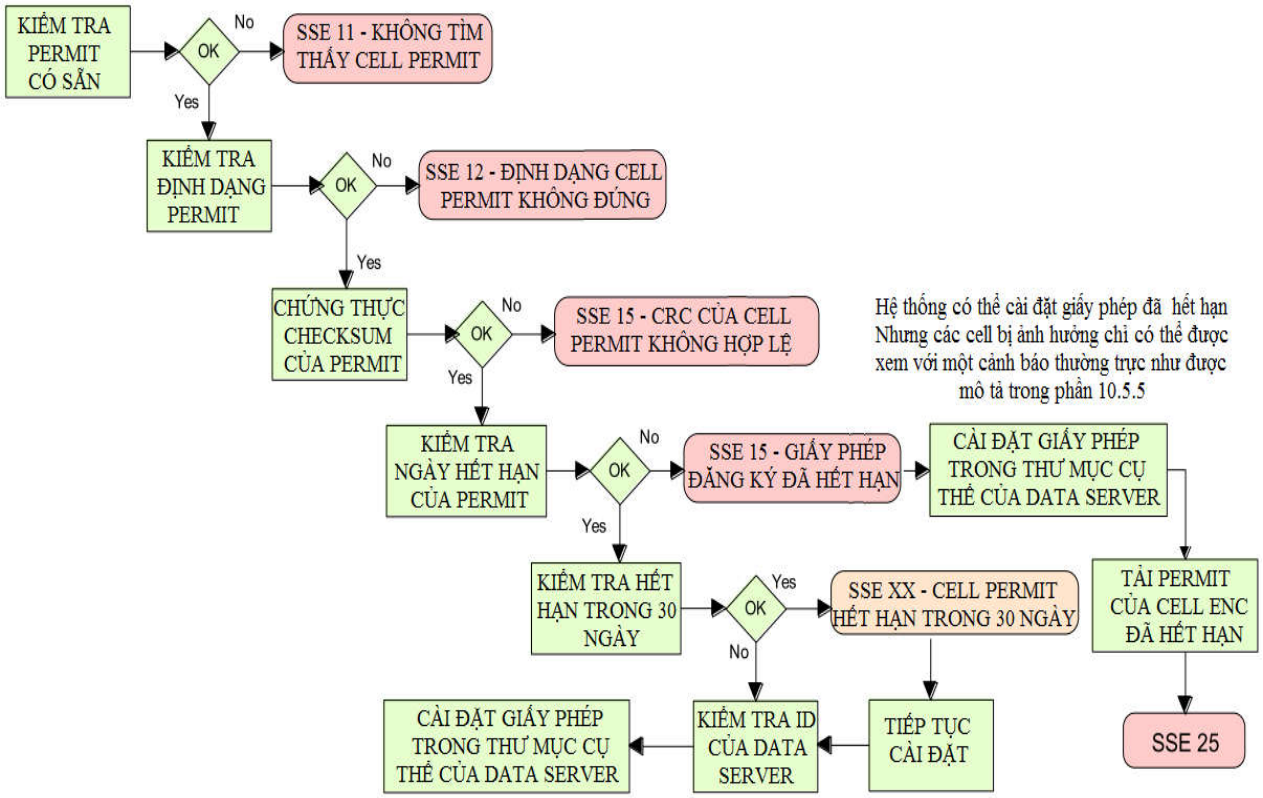
10.5.6 Kiểm tra ID của Data Server.

Lược đồ bảo vệ dữ liệu S-63 tính đến môi trường nhiều nhà cung cấp, đó là lúc Data Client thu được giấy phép từ nhiều hơn 1 Data Server. Có vài trường hợp Data Clients có dữ liệu ENC từ nhiều nhà cung cấp như sau:

- Các cell trùng nhau được cấp phép từ các Data Server khác nhau.
- Thay đổi từ Data Server này sang Data Server khác.

Điều quan trọng là hệ thống Data Client có thể quản lý các trường hợp này.Mỗi bản ghi giấy phép chứa một trường ID của Data Server (xem phần 4.3.3).Trường này, nếu được tích vào, chứa hai ký tự chữ và số ID duy nhất cho mỗi Data Server được gán bởi SA.Kể từ khi Cell Permit được phát hành bởi một Data Server việc giải mã các ENC được cung cấp mởi một Data Server khác không quan trọng bằng việc duy trì mối liên kết giữa giấy phép và ENC đã mã hóa. OEM nên đảm bảo rằng hệ thống của họ có khả năng duy trì sự liên kết này, ví dụ bằng cách tạo các thư mục cụ thể cho Data Server, nơi các giấy phép được lưu trữ.

ID Data Server cho Bộ sản phẩm trao đổi ENC đã mã hóa chứa trong tập tin SERIAL.ENC (xem phần 6.3.1) và trùng với ID chứa trong bản ghi Cell Permit.



Hệ thống OEM - Cài đặt và chứng thực hệ thống OEM

10.6 Kiểm tra tính toàn vẹn và xác thực ENC

Hệ thống OEM phải có khả năng chứng thực nguồn gốc dữ liệu ENC đã mã hóa và xác thực tính toàn vẹn của nó. Điều này đạt được bằng 2 cách sau:

- Bằng cách chứng thựcchữ ký SA được tổ chức như một phần của Chứng chỉ Data Server là một phần của tập tin Chữ ký số ENC.
- Bằng cách chứng thực Chữ ký ENC của Data Server (tương ứng với dữ liệu cell ENC) trong tập tin Chữ ký ENC.

OEM và Data Client trước hết phải xác nhận rằng chứng chỉ SA (định dạng X509 hoặc ASCII) được cài đặt trên ECS/ECDIS là hiện cóvàchính xác. Điều này được đề cập trong phần 10.6.1 dưới đây.

10.6.1 Xác thực/xác minh Chứng chỉ số SA

Thủ tục này được thực hiện bởi các OEM hoặc Data Client để xác minh rằng khóa chung SA được cài đặt trên ECS/ECDIS là chính xác và tuân thủ Lược đồ bảo vệ Dữ liệu IHO S-63. Nó là khóa chung SA sử dụng để xác thực Chứng chỉ Data Server được SA ký được cung cấp bởi Data Server như là một phần của tập tin chữ ký ENC. Thủ tục như sau:

So sánh thủ công khóa chung SA chứa trong Chứng chỉ số SA được cài đặt độc lập với một bản sao của khóa chung in sẵn từ website của IHO (http://www.iho.int). Nếu kiểm tra trên bị lỗi, hệ thống sẽ không chấp nhận Chứng chỉ số SA. Ngược lại, chứng chỉ số SA là hợp lệ và Khóa chung của Data Server chứa nó có thể được sử dụng để xác nhận Chứng chỉ Data Server được SA ký như là một phần của tập tin chữ ký ENC.

LƯU Ý: Data Client phải có phương pháp mà người dùng có thể truy cập

vào chứng chỉ được cài đặt từ ứng dụng.

10.6.1.1 Kiểm tra bằng tay Khóa chung SA.

Khóa chung SA có thể được truy cập từ trang Web IHO như sau:

"http://www.iho.int→ Home → Publications → Download List → S-63 → S-63 SA Certificate"

Trang web sau sẽ được hiển thị:

CHỨNG CHỈ SỐ S-63 (S-63 DIGITAL CERTIFICATES)

Chứng chỉ số là tập tin ràng buộc một khóa chungcụ thể cùng các thông tin khác tới một cá nhân hoặc tổ chức.Tiêu chuẩn S-63 sử dụng một chuỗi 2 cấp độ của chứng chỉ để vận hành lược đồ bảo vệ dữ liệu.

IHBhoạt động như một Nhà quản trị Lược đồ và phát hành các Chứng chỉ số gốc để sử dụng trong Lược đồ bảo vệ.Chứng chỉ SA được sử dụng bởi IHB sẽ là một Chứng chỉ tự ký. Nó có sẵn cả hai dạng như tập tin theo X-509 là ***IHO.CRT*** *và như một tập tin văn bản****Scheme Administrator Public Key.txt (Khóa chung của Nhà quản trị lược đồ.txt).*** *Cả hai tập tin chứa trong một tập tin nén là* ***SA Certificate****(Chứng chỉ SA).*

SA sẽ phát hành Chứng chỉ Data Server tới tất cả các Data Server tham gia vào Lược đồ bảo vệ. Chứng chỉ Data Server chứa Khóa chungData Server và Chữ ký SA của khóa này. Vì chỉ có SA có thể phát hành Chứng chỉ Data Server, một chuỗi sự tin tưởng có thể được thiết lập bằng cách xác thực Chữ ký SA trên Khóa chung Data Server.

Lược đồ bảo vệ yêu cầu khóa chung SA phải được cài đặt trên hệ thống người dùng cuối bởi tất cả người dùng lược đồ bảo vệ. Chứng chỉ Data Server chứa trong mỗi tập tin chữ ký và khóa chung Data Server có thể được tin cậy nếu chứng chỉ SA là hợp lệ. Việc cài đặt chứng chỉ SA (và khóa chung chứa bên trong) nên được thực hiện riêng rẽ, hoạt động độc lập và chịu sự kiểm soát cẩn thận của các thủ tục điều hành.

Trong đoạn thứ 2 ở trên, nhấn vào "***SA Certificate"*** và một hộp thoại **"File Download"** sẽ hiển thị nhằm cung cấp cho người dùng tùy chọn "**Mở**" hoặc "**Lưu**"một tập tin nén có tên "**S-63_SA_Certificate.zip**". Tập tin này chứa 2 tập tin khác như sau:

1. IHO.CRT (Chứng chỉ X509)

Mở tập tin này xuất hiện một hộp thoại "***Certificate***", lựa chọn tab "**Details**" và làm nổi bật "**Public Key– Khóa chung**" để hiển thị Khóa chung IHO. Ví dụ dưới đây là Khóa chung IHO tại thời điểm tài liệu này được công bố. Lưu ý rằng 4 hoặc 6 ký tự đầu tiên [024100] đại diện cho các tham số của Chứng chỉ và có thể dương [0240] hoặc âm [024100].

```
0241 0096 3F14 E32B A537 2928 F24F 15B0 730C
49D3 1B28 E5C7 6410 0256 4DB9 5995 B15C F880
0ED5 4E35 4867 B82B B959 7B15 8269 E079 F0C4
F492 6B17 761C C89E B77C 9B7E F8
```

Chuỗi ký tự này (trừ các tham số của Chứng chỉ) nên được so sánh với Chứng chỉ đã cài đặt để xác nhận rằng chúng là như nhau.Nếu giống nhau, chứng chỉ được xác thực, nếu không giống nhau thì chứng chỉ sẽ bị hủy bỏ.

2 Khóa chung của Nhà quản trị lược đồ.txt (Scheme Administrator

Public Key.txt)

Mở tập tin này sẽ hiển thị các tham số của Khóa chung SA như sau:

// BIG p
FCA6 82CE 8E12 CABA 26EF CCF7 110E 526D B078 B05E DECB CD1E B4A2 08F3 AE16 17AE
01F3 5B91 A47E 6DF6 3413 C5E1 2ED0 899B CD13 2ACD 50D9 9151 BDC4 3EE7 3759 2E17.
// BIG q
962E DDCC 369C BA8E BB26 0EE6 B6A1 26D9 346E 38C5.
// BIG g
6784 71B2 7A9C F44E E91A 49C5 147D B1A9 AAF2 44F0 5A43 4D64 8693 1D2D 1427 1B9E
3503 0B71 FD73 DA17 9069 B32E 2935 630E 1C20 6235 4D0D A20A 6C41 6E50 BE79 4CA4.
// BIG y
963F 14E3 2BA5 3729 28F2 4F15 B073 0C49 D31B 28E5 C764 1002 564D B959 95B1 5CF8
800E D54E 3548 67B8 2BB9 597B 1582 69E0 79F0 C4F4 926B 1776 1CC8 9EB7 7C9B 7EF8.

Nếu tập tin này được sử dụng để xác thực, nó sẽ được kiểm tra dựa vào tập tin chứng chỉ hoặc Khóa chung đã được cài đặt. Nếu việc kiểm tra dựa vào một Chứng chỉ đã cài đặt, sau đó chỉ có chuỗi "**BIG y**" cần được xác minh để xem xét nếu nó giống nhau. Nếu kiểm tra dựa vào tập tin Khóa chung thì sau đó tất cả các tham số phải được xác minh để xem xét nếu nó giống nhau. Trong cả hai trường hợp, nếu tập tin đúng, sau đó khóa chung được xác thực, nếu không nó phải bị gỡ bỏ.

10.6.2 Xác thực Chứng chỉ Data Server được SA ký

Thủ tục này được thực hiện bởi hệ thống Data Server nhằm xác nhận Chứng chỉ Data Server được SA ký được lưu trữ như là một phần của tập tin Chữ ký ENC dựa vào Khóa chung SA đã cài đặt. Quá trình này thực hiện trước khi Khóa chung Data Server được trích xuất để xác thực Chữ ký ENC. Tham khảo phần 5.3.2 về Cấu trúc cặp Chữ ký/Chứng chỉ trong một tập tin Chữ ký.

Trước khi thực hiện xác thực thì hệ thống phải kiểm tra tính sẵn có, định dạng và trạng thái của Chứng chỉ hoặc Khóa chung được cài đặt trên hệ thống. Nếu có bất cứ vấn đề gì thì hệ thống cần thông báo cho Data Client bằng cách đầy ý nghĩa như sau:

1. Chứng chỉ SA hoặc Khóa chung hiện không có trên hệ thống (**SSE 05** và kết thúc quá trình).
2. Định dạng Chứng chỉ SA hoặc Khóa chung không chính xác (**SSE 08** và kết thúc quá trình).
3. Chứng chỉ SA đã hết hạn (**SSE 22** và kết thúc quá trình).

Thủ tục xác nhận như sau:

a) Giải nén tập tin Chữ ký ENC.

b) Loại bỏ phần chữ ký đầu tiên (tức là hai chuỗi dữ liệu đầu tiên và phần tiêu đề kèm theo của nó. Đây là Chữ ký Data Server của dữ liệu ENC). Việc này thu về Chứng chỉ Data Server được SA ký.

c) Trích xuất phần còn lại của chữ ký (tức là hai chuỗi dữ liệu đầu tiên và phần tiêu đề kèm theo của chúng từ tập tin còn lại thu được từ 'b'). Việc này thuvề một tập tin Khóa chung.

d) Băm tập tin Khóa chung (thu được từ 'c') bằng cách sử dụng thuật toán SHA-1 [3]. Tất cả các byte bên trong tập tin đều được băm.

e) Xác minh phần Chữ ký (bị loại bỏ ở mục 'c') bằng cách thông qua nó

(Chữ ký), cùng với tập tin Khóa chung SA (khóa) và băm của tập tin Khóa chung (thu được từ 'd') tới DSA [2]. Việc này trả về một trạng thái (đúng hoặc không đúng).

Nếu không đúng thì hệ thống kết thúc quá trình và trả về cảnh báo sau:

"SSE 06 - "The SA Signed Data Server Certificate is invalid. The SA may have issued a new public key or the ENC may originate from another service. A new SA public key can be obtained from the IHO website or from your data supplier" – *"SSE 06 – Chứng chỉ Data Server được SA ký không hợp lệ. SA có thể đã phát hành một khóa chung mới hoặc ENC có thể sinh ra từ một dịch vụ khác. Có thể thu về Khóa chung SA mới từ trang web IHO hoặc từ nhà phân phối dữ liệu".*

10.6.2.1 Xác nhận chống lại Chứng chỉ Data Server không phải SA ký

Có thể có trường hợp có nhiều hơn 1 chứng chỉ hoặc khóa chung được lưu trữ trên Data Client. Điều này có thể đặt biệt trong suốt quá trình chuyển đổi để sử dụng đúng lược đồ S-63.Vì vậy việc kiểm tra là cần thiết để bảo đảm rằng Chứng chỉ Data Server xác thực một cách chính xác IHO.CRT hoặc IHO.PUB cài đặt trên Data Client.

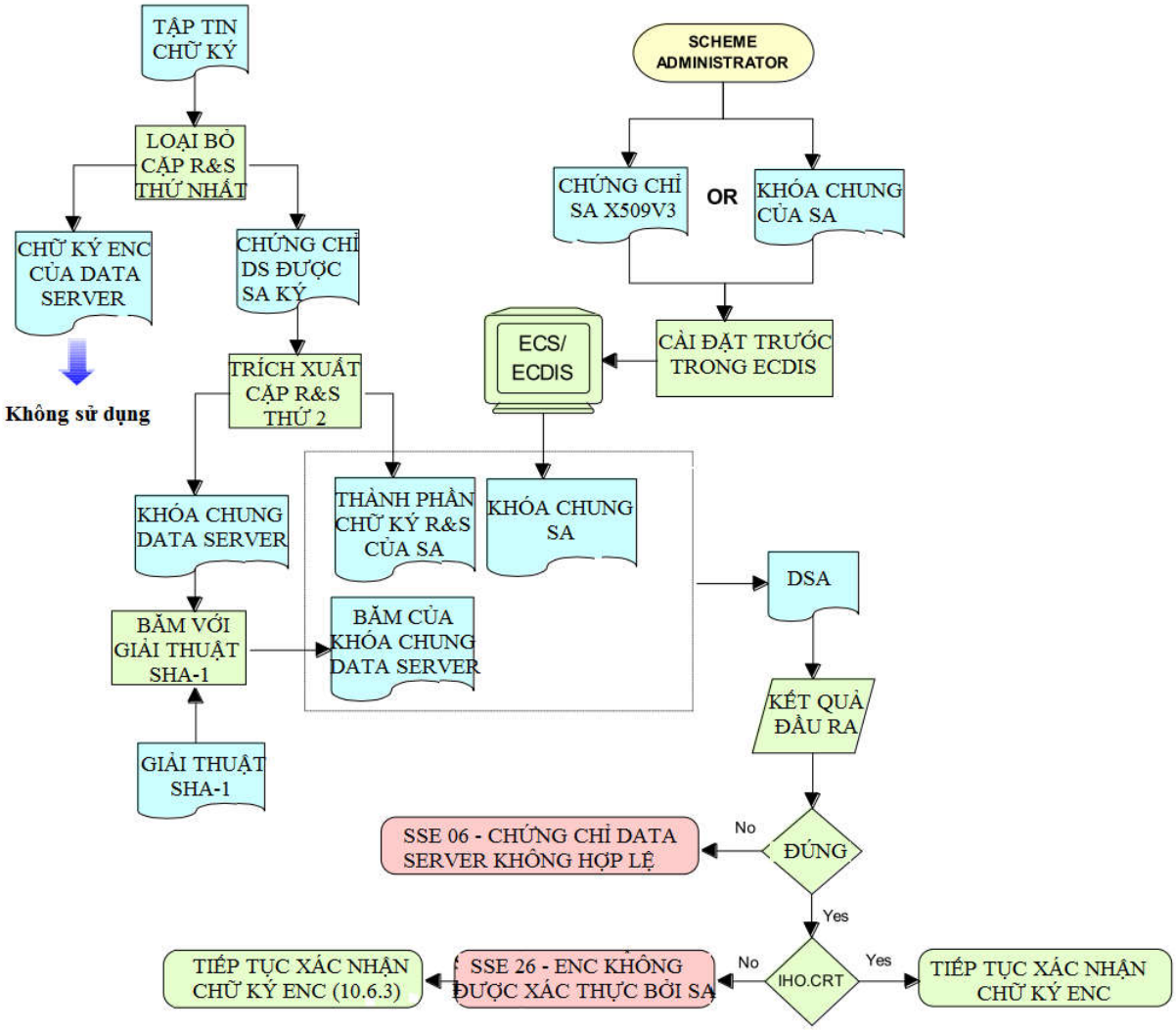
Nếu Chứng chỉ Data Server xác thực không dựa vào IHO.CRT hoặc IHO.PUB được lưu trữ trên Data Client thì sau đó **PHẢI** có cảnh báo được hiển thị như sau:

"SSE 26 - "This ENC is not authenticated by the IHO acting as the Scheme Administrator" – *"SSE 26 – ENC này không được xác thực bởi IHO (tức là Nhà quản trị lược đồ)".*

Việc này chỉ cần thiết cho Data Client khi hiển thị cảnh báo này và không xuất hiện lặp lại cho các lỗi tương tự trong Bộ Sản phẩm trao đổi. Nếu tin nhắn này được hiển thị thì Data Client sẽ vẫn tiếp tục bướctiếp theo của việc xác thực (xác thực chữ ký ENC) và việc giải mã.

10.6.3 Xác thực tập tin Cell ENC

Thủ tục này được thực hiện bởi hệ thống Data Client để xác nhận chữ ký ENC (được tổ chức trong tập tin Chữ ký ENC) tương ứng với tập tin Cell ENC cụ thể.Người ta hy vọng rằngData Client đã thực hiện các thủ tục để xác thực Chứng chỉ số SA (phần 10.6.1) và Chứng chỉ Data Server bên trong tập tin Chữ

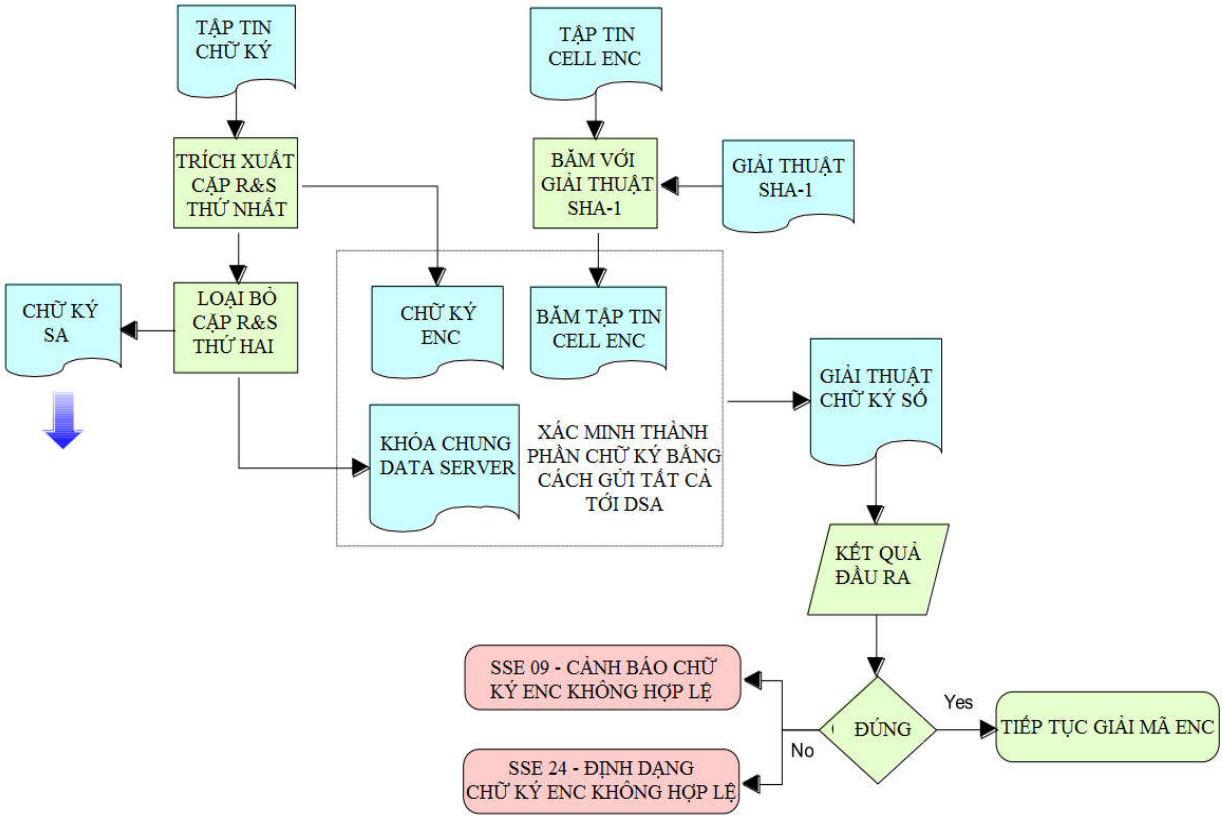


Chứng chỉ Data Server được SA ký

ký (phần 10.6.2). Thủ tục để xác thực tập tin Cell ENC như sau:

a) Giải nén tập tin chữ ký ENC duy nhất liên quan tới tập tin cell ENC.
b) Trích xuất phần đầu tiên của Chữ ký (tức là hai chuỗi dữ liệu đầu tiên và tiêu đề kèm theo của nó). Việc này để lại Chứng chỉ.
c) Loại bỏ phần chữ ký còn lại (tức là hai chuỗi dữ liệu đầu tiên và tiêu đề kèm theo từ phần còn lại của tập tin). Việc này để lại tập tin Khóa chung.
d) Băm tập tin cell ENC được liên kết bằng cáchsử dụng thuật toán SHA-1 [3]. Tất cả các byte bên trong tập tin đều được băm.
e) Xác minh phần Chữ ký (được trích xuất từ mục 'b') bằng cách thông qua nó (chữ ký), khóa chung - phía bên trái mục 'c' (khóa) và băm của tập tin Cell ENC, thu được tại mục 'd'tới DSA [2]. Thao tác này trả về một trạng thái (đúng hoặc không đúng).

Nếu chữ ký ENC không được xác thực chính xác, Data Client sẽ không giải mã ENC vì nguồn gốc của nó không được xác minh. Nếu ENC được xác thực chính xác, thì ENC an toàn để giải mã.



Xác thực tập tin cell ENC - Xác nhận chữ ký ENC

10.7 Giải mã tập tin dữ liệu ENC Base và ENC Update.

Trước khi giải mã tập tin Cell ENC base và update mới thì hệ thống trước tiên nên kiểm tra trạng thái đăng ký của Cell Permit được cài đặt. Quá trình này nhằm xác định xem liệu Data Client có được phép nhận và cài đặt dữ liệu ENC mới.Hệ thống này cũng tìm cách cung cấp đầy đủ các cảnh báo cho Data Client trước khi giấy phép hết hạn.

10.7.1 Kiểm tra tình trạng đăng ký của các giấy phép được cài đặt.

Phần 10.5 xác địnhcác quy trình và kiểm tra được thực hiện bởi Hệ thống Data Client khi cài đặt Cell Permit.Phần này xác định làm cách nào để các Cell Permit được quản lý bởi hệ thống Data Client khi được cài đặt.Nó cũng được thiết kế để cung cấp cho Data Client các cảnh báo nâng cao vềgiấy phép đăng ký sắp hết hạn, đặc biệt là khi dữ liệu ENC được sử dụng cho hàng hải.

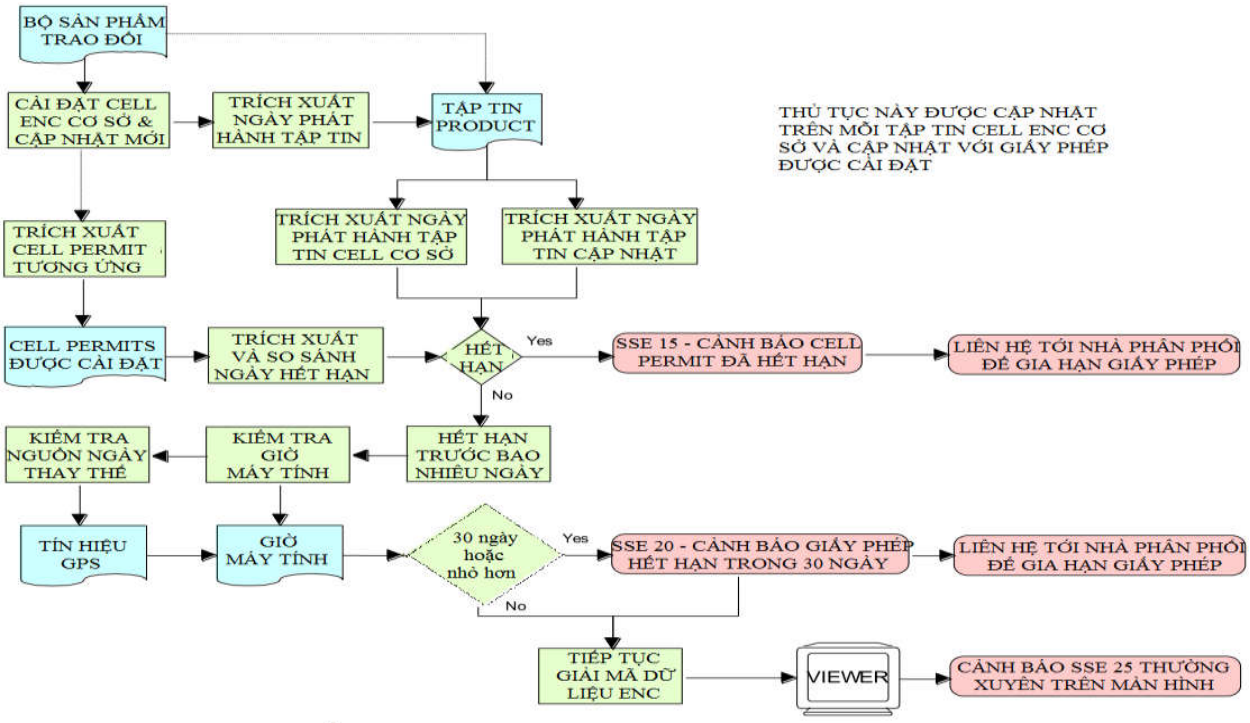
10.7.1.1 Kiểm tra nếu đăng ký đã hết hạn trong Cell Permit - Cảnh báo bắt buộc

Việc kiểm tra này được thực hiện trên các tập tin Cell ENC cơ sở và cập nhật mới trước khi giải mã.Việc kiểm tra này là cần thiết để thông báo cho Data Client rằng giấy phép đăng ký đã hết hạn nhưng các cell ENC Updates/base đã sẵn có.Cảnh báo này chỉ áp dụng cho giấy phép đăng ký và không được sử dụng cho các giấy phép mua lẻ, tham khảo phần 4.3.3.Thủ tục này được tóm lược trong sơ đồ tiến trình phía dưới và tiếp đến là miêu tả từng bước.

a) Trích xuất ngày hết hạn của Cell Permit được tải lên tương ứng với tập tin ENC đã mã hóa.
b) Trích xuất ngày phát hành của tập Cell ENC cơ sở và bản cập nhật mới nhất (nếu sẵn có[12]) được giải mãtừ tập tin PRODUCTS.TXT. Thông tin này nằm ở trường thứ 2 (ngày phát hành sản phẩm) và trường thứ 4 (ngày phát hành bản cập nhật mới nhất) của bản ghi cell tương ứng với cell được mã hóa.
c) Nếu 2 ngày (trong trường 2 và trường 4) được trả về tại mục 'b' sau đó chỉ ngày gần nhất[13] được sử dụng để kiểm tra với ngày hết hạn.
d) Nếu ngày phát hành của cell Base hoặc cell Update thu được tại b) và c) là mới hơn (trước) ngày giấy phép hết hạn thu được tại a) thì giấy phép bị cho là đã hết hạn. Một cảnh báo phải được hiển thị như sau:

"SSE 15 - Subscription service has expired. Please contact your data supplier to renew the subscription licence." *"SSE 15- Dịch vụ đăng ký đã hết hạn.Vui lòng liên hệ với nhà phân phối dữ liệu đểgia hạn giấy phép đăng ký".*

Ứng dụng có thể **<u>cài đặt giấy phép ENC đã hết hạn</u>** nhưng phải hiển thị cảnh báo "**SSE 15**" như trên.Nó cũng có thể giải mã tập tin Cell ENC base và update trước ngày hết hạn giấy phép.Điều này có thể được quản lý bằng cách sử dụngNgày phát hành [ISDT] chứa trong trường CATD-COMTlúc nhập vào.Không nên nhập vào cell cơ sở hoặc cập nhật nếu ngày phát hành [ISDT] lớn hơn ngày hết hạn của Cell Permit được cài đặt.Ứng dụng cũng phải hiển thị một cảnh báo thường xuyên khi giấy phép sử dụng cell hết hạn trong Data Client, xem mục10.8.1



Quy trình kiểm tra tình trạng đăng ký trước khi giải mã

[12]Nếu không có bản cập nhật đã phát hành cho một cell thì không có thông tin sẵn có.
[13]Trường "Ngày phát hành bản cập nhật mới nhất", nếu được tích, sẽ không thể trước "Ngày phát hành sản phẩm", ví dụ trong trường hợp phát hành lại.

10.7.1.2 Kiểm tra tình trạng sử dụng - yêu cầu cảnh báo trước 30 ngày

Việc kiểm tra này phải được thực hiện khi tập tin cell ENC cơ sở hoặc cập nhật mới được cài đặt và phải thông báo cho Data Client trạng thái về tình trạng giấy phép đăng ký trước ngày hết hạn. Mục đích là đảm bảo cho Data Client có thời gian gia hạn giấy phép đăng ký của họ và thu về Cell Permit được cập nhật từ Data Server. Cảnh báo chỉ áp dụng cho giấy phép đăng ký và không áp dụng cho giấy phép mua đơn lẻ, tham khảo phần 4.3.3. Thủ tục như sau:

a) Thu được ngày hệ thống và nếu có thể, thu thêm các thông tin thời gian đáng tin cậy khác, ví dụ tín hiệu GPS.
b) Thu được ngày hết hạn đăng ký từ tập tin Cell Permit.
c) So sánh ngày hệ thống từ 'a' và ngày hết hạn đăng ký từ 'b'.
d) Nếu nó nhiều hơn 30 ngày trước ngày hết hạn đăng ký, hệ thống có thể hoạt động mà không cần thông báo thêm cho người dùng.
e) Nếu ít hơn 30 ngày trước ngày hết hạn đăng ký, hệ thông có thể giải mã và giải nén thông tin mới được phát hành trong thời gian đăng ký. Hệ thống sẽ ban hành một thông điệp cảnh báo tới người dùng như sau:

"SSE 20 - Subscription service will expire in less than 30 days. Please contact your data supplier to renew the subscription licence." *–"Dịch vụ đăng ký sẽ hết hạn trong vòng chưa đầy 30 ngày.Vui lòng liên hệ với nhà phân phối dữ liệu để gia hạn giấy phép".*

10.7.2 Giải mã Cell Key trong Cell Permit

Thủ tục này được thực hiện bởi hệ thống Data Client sau khi hoàn thành xác thực tập tin Chữ ký ENC. Quá trình giải mã bắt đầu bằng việc trích xuất cell key cần thiết để giải mã ENC, bao gồm các bước sau:

a) Gắn byte đầu tiên của HW_ID Data Client vào cuối HW_ID để được dạng HW_ID 6 byte (gọi là HW_ID6).
b) Trích xuất ECK1 từ Cell Permit và chuyển đổi ECK1 từ chuỗi 16 ký tự hex thành 8 byte.
c) Giải mã ECK1 đã chuyển đổi (đầu ra từ 'b') bằng cách sử dụng thuật toán Blowfish với HW_ID là chìa khóa. Điều này trả về CK1.
d) Trích xuất ECK2 từ Cell Permit và chuyển đổi ECK2 này từ dạng chuỗi 16 ký tự hex thành 8 byte.
e) Giải mã ECK2 đã chuyển đổi (đầu ra từ 'd') bằng cách sử dụng thuật toán Blowfish với HW_ID6 là chìa khóa. Điều này sẽ trả về CK2.

Ví dụ:

HW_ID	3132333438	Dạng Hex
Cell Permit	NO4D061320000830BEB9BFE3C7C6CE68 B16411FD09F96982795C77B204F54D48	Ví dụ về Cell Permit

Đầu ra từ 'a'	313233343831	HW_ID6
Đầu ra từ 'b'	8 byte – không in được	ECK1 đã mã hóa
Đầu ra từ 'c'	C1CB518E9C	Cell Key 1 (dạng hex)
Đầu ra từ 'd'	8 byte – không in được	ECK2 đã mã hóa
Đầu ra từ 'e'	421571CC66	Cell Key 2 (dạng hex)

Lưu ý rằng các Cell Key không được mã hóa có chiều dài 5 byte, mặc dù

cácCell Key được mã hóa có chiều dài 8 byte. Điều này là do thuật toán Blowfish đệm thêm vào Cell Key để có chiều dài 8 byte khi mã hóa chúng và không đệmthêm vào cell key mã hóa khi giải mã chúng.

10.7.3 Giải mã tập tin cell ENC cơ sở hoặc cập nhật

Thủ tục này được thực hiện bởi hệ thống Data Client và được thực hiện như nêu trong biểu đồ tiến trình (xem phần 10.7.2 và 10.7.3) và sau đây là hướng dẫn từng bước[14]:

a) Giải mã tập tin ENC bằng cách sử dụng thuật toán Blowfish với CK1 là khóa giải mã[15].
b) Giải nén tập tin ENC. Nếu giải nén thành công thì tập tin ENC được giải mã và sẵn sàng để nhập vào.
c) Nếu giải nén không thành công, giải mã tập tin ENC bằng cách sử dụng thuật toán Blowfish với CK2 là khóa giải mã.
d) Giải nén tập tin ENC. Nếu giải nén thành công, tập tin ENC được giải mã và sẵn sàng để sử dụng.
e) Nếu giải nén không thành công ở mục 'b' và 'd', điều này có nghĩa Cell Permit không chứa giá trị cell key hợp lệ. Hệ thống sẽ trả về một thông điệp cảnh báo phù hợp và thông báo cho Data Client rằng một Cell Permit mới đượcthu về từ Data Server.

"SSE 21 – Decryption failed no valid cell permit found. Permits may be for another system or new permits may be required, please contact your supplier to obtain a new licence." – *"SSE 21- giải mã thất bại do không tìm thấy cell permit hợp lệ. Giấy phép có thể cho hệ thống khác hoặc giấy phép mới có thể được yêu cầu, vui lòng lên hệ với nhà phân phối dữ liệu để thu về giấy phép mới".*

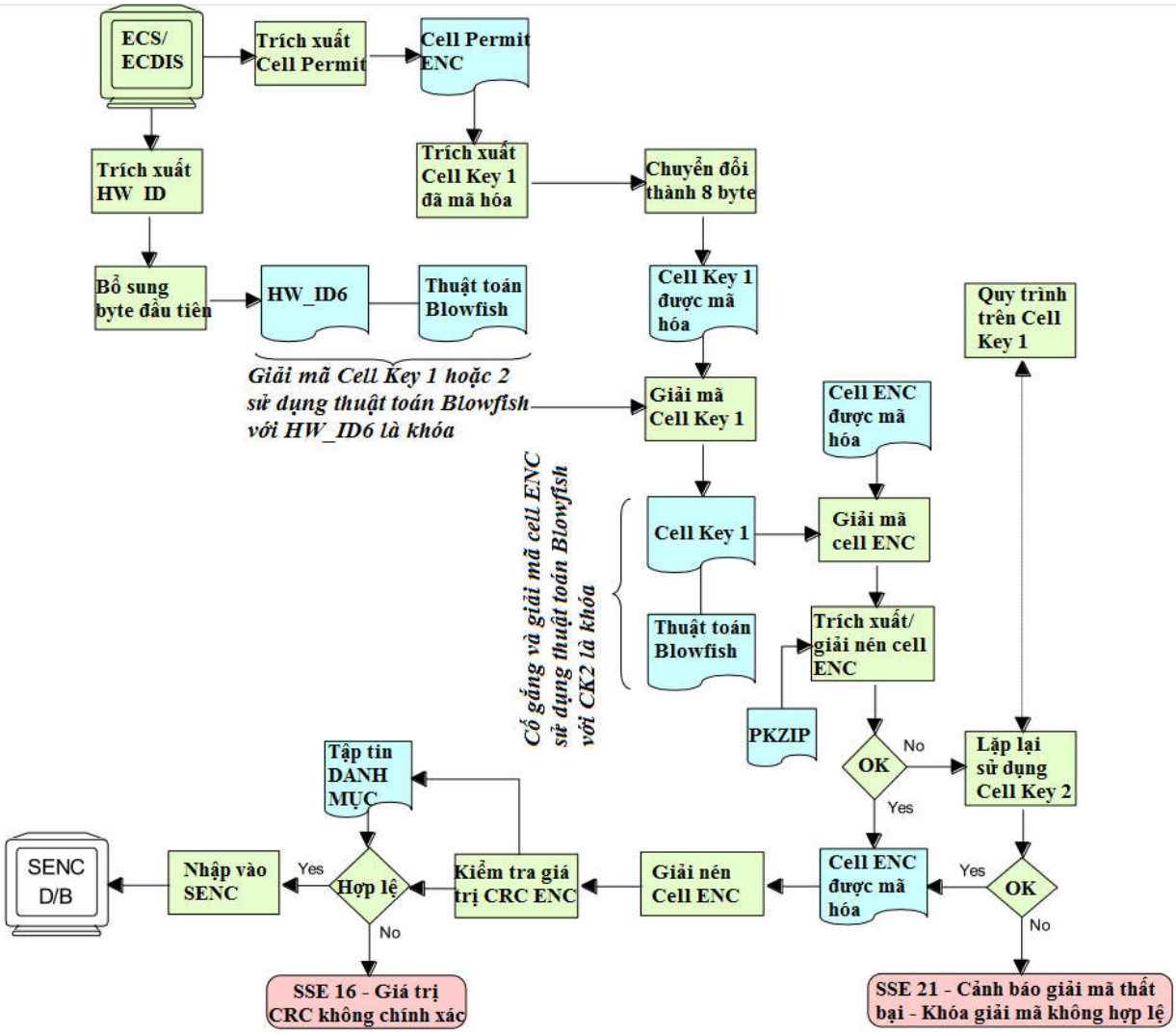
10.7.4 Giải nén tập tin ENC (base hoặc Update)

Thủ tục này được thực hiện bởi Data Client khi giải mã tập tin ENC. Thủ tục này như sau:

Giải nén tập tin ENC bằng cách sử dụng tiêu chuẩn ZIP [6] để tạo một tập tin hoàn toàn tuân thủ Tiêu chuẩn S-57 Ấn bản 3.1- Chi tiết kỹ thuật sản phẩm ENC.

LƯU Ý: Giá trị CRC của ENC [1] luôn được tính trên thông tin ENC không được mã hóa. Ứng dụng phải xác nhận việc giải mã và giải nén thành công bằng cách tiến hành kiểm ra CRC trên tất cả thông tin ENC.

[14]OEM nên lưu ý rằng không có yêu cầu để kiểm tra ngày ấn bản dựa vào giấy phép hoặc từ thủ tục này.
[15] Thay vì giải mã và giải nén toàn bộ tập tin ENC, Data Client có thể kiểm tra thông tin tiêu đề được giải mã phù hợp với tiêu chuẩn ZIP [6].



Giải mã và giải nén tập tin cell ENC Base và Update

10.8 Các cảnh báo thường xuyên trên Data Client

Data Client đã thực hiện kiểm tra khi tải tập tin dữ liệu và giấy phép ENC để xác nhận sự phù hợp với tiêu chuẩn này.Tuy nhiên, bất kỳ kết quả lỗi hoặc thông điệp cảnh báo có thể khôngđược dịch thông qua ECDIS khi nó đang sử dụng, ví dụ khi lập tuyến hành trình hoặc điều hướng. Điều đó là có thể, theo Lược đồ bảo vệ dữ liệu hiện tại, sử dụng các ENC đã lỗi thời mà người dùng không biết rõ điều đó. Mục đích của phần này là để nhận biết các thông báo sẽ thường xuyên được hiển thị bằng Data Client khi đang sử dụng.

Data Client phải hiển thị thông điệp cảnh báo thường xuyên cho người xem khi nó được xác định rằng thông tin ENC chứa trong SENC đã lỗi thời.Data Client phải thực hiện việckiểm tra sau đây khi hiển thị một cell trên ECDIS:

- Có giấy phép ENC cài đặt hết han?
- Có phải dữ liệu SENC được cài đặt lỗi thời đối với tập tin PRODUCTS.TXT được cài đặt mới nhất?

10.8.1 Giấy phép ENC hết hạn

Data Client phải kiểm tra tình trạng của giấy phép ENC được cài đặt khi hiển thị một cell ENC cụ thể. Nếu giấy phép đã hết hạn thì ECDIS hiển thị một cảnh báo thường xuyên thông báo cho người dùng rằng cell ENC này có thể đã

lỗi thời như sau:

"SSE 25 - The permit for ENC<cell name> has expired. This cell may be out of date and MUST NOT be used for Primary NAVIGATION". – *"SSE 25 – giấy phép cho ENC <tên cell> đã hết hạn.Cell này có thể đã lỗi thời và KHÔNG ĐƯỢC sử dụng cho HÀNG HẢI".*

10.8.2 Dữ liệu SENC lỗi thời

Data Client phải kiểm tra tình trạng của cell ENC được hiển thị dựa vào trạng thái đã biết của các cell trong một dịch vụ của Data Server riêng. Điều này phải được thực hiện bằng cách so sánh phiên bản hiện tại [EDTN] và Cập nhật [UPDN] chứa trong hệ thống SENC cho tất cả các cell dựa vào bản ghi cell tương ứng được liệt kê trong tập tin PRODUCTS.TXT mới nhất.

Một cảnh báo thường xuyên được đưa ra khi cell ENC hiển thị bởi ECDIS không được cập nhật phiên bản hoặc bản cập nhật mới nhất trong dịch vụ như sau:

"SSE 27 - ENC<cell name> is not up to date. A New Edition, Re-issue or Update for this cell is missing and therefore MUST NOT be used for Primary NAVIGATION". – *"SSE 27 – ENC <tên cell> không được cập nhật. Một phiên bản mới, dữ liệu tái bản hoặc bản cập nhật bị thiếu, dó dó KHÔNG ĐƯỢC sử dụng cho mục đích HÀNG HẢI".*

10.9 THỦ TỤC QA – DATA CLIENT

10.9.1 Kiểm tra và chấp nhận Chứng chỉ số SA (và Khóa chung)

Data Server sẽ nhận khóa chung của SA ở 2 định dạng, dạng chứng chỉ số X.509 và dạng khóa chung in ra được. Data Client sẽ có khả năng tải Chứng chỉ số SA và so sánh bằng tay khóa chung dựa vào khóa chung được in ra (xem phần 10.6.1.1). Data Client sẽ chỉ chấp nhận khóa chung của SA khi điều này đã được thực hiện. Quy trình này áp dụng cho các Khóa chungđầu tiêncủa SA và bất cứ khóa chung tiếp theo được SAphát hành.

10.9.2 Tạo User Permit

Nhà cung cấp Hệ thống/ứng dụng có khả năng tạo User Permit riêng của họ chứa HW_ID đã mã hóa.User Permit được cung cấp cho Data Server để tạo Cell Permit cho thông tin ENC được yêu cầu.User Permit sẽ chỉ được tạo để yêu cầu Cell Permit từ Data Server.

10.9.3 Xác nhận Chứng chỉ Data Server

Nhà sản xuất ứng dụng sẽ cho phép xác minh Chứng chỉ Data Server chứa trong tập tin Chữ ký ENC bằng cách sử dụng Khóa chung SA. Nếu Chứng chỉ Data Server được xác minh thành công, ứng dụng sau đó sẽ trích xuất Khóa chung Data Server từ Chứng chỉ Data Server và sử dụng nó để xác minh Chữ ký ENC.

SA sẽ thông báo cho Nhà Sản xuất về việc thu hồi Chứng chỉ Data Server.

10.9.4 Xác nhận Cell Permit

Hệ thống Data Client phải có khả năng để xác nhận tính toàn vẹn của Cell Permit bằng cách kiểm tra Check Sum đã mã hóa. Điều này được thực hiện bằng cách thực hiện theo các thủ tục quy định trong phần 10.5.4 của Chi tiết kỹ thuật.

Data Client phải có khả năng quản lý Cell Permit được cung cấp bởi nhiều Data Server.Data Client cũng phải có khả năng quản lý Cell Permit của các ENC giống nhau được cung cấp bởi nhiều Data Server.

Data Client phải có khả năng quản lý các Cell Permit được lưu trữ sao cho

các Cell Permit cũ có thể bị xóa bỏ và các Cell Permit mới được thêm vào hoặc hợp nhất với các Cell Permit đã được lưu trữ.

Ứng dụng Data Client không nên cho phép Data Client có khả năng xem được hoặc sao chép các Cell key đã mã hóa.

10.9.5 Xác nhận và giải mã thông tin ENC

Data Client phải có khả năng chấp nhận một tập dữ liệu ENC được ký và được mã hóa bằng cách làm theo thủ tục được định rõ trong phần 10.6 và 10.7.

10.10 Các thủ tục QA – Nhà sản xuất ECDIS (OEMs)

10.10.1 Thỏa thuận bảo mật

SA sẽ cung cấp cho Nhà sản xuất bản sao tất cả thông tin được yêu cầu để vận hành Lược đồ bảo vệ dữ liệu trong một Thỏa thuận bảo mật. Nhà sản xuất phải tuân thủ các điều khoản và điều kiện của Thỏa thuận bảo mật và đảm bảo rằng tất cả thông tin cung cấp được lưu giữ đến nay.

10.10.2 Kiểm tra tuân thủ hệ thống

Nhà sản xuất ECDIS sẽ thực hiện kiểm tra sự tuân thủ nội bộviệc tuân thủ đầy đủ Lược đồ bảo vệ, trên cơ sở các mô tả được cung cấp trong tài liệu này và dữ liệu thử nghiệm được cung cấp.

SA sẽ chỉ phát hành M_ID và M_KEY khi kiểm tra sự tuân thủ thành công như được cung cấp bởi một tài liệu chứng chỉ tự ký.

10.10.3 Lưu trữ M_ID và M_KEY

Khi Nhà sản xuất ECDIS tham gia Lược đồ, SA sẽ cung cấp thông tin thuộc tính để tạo User Permit.

Người sử dụng ứng dụng của Nhà sản xuất ECDIS không thể xem hoặc trích xuất thông tin M_KEY.

10.10.4 Tạo HW_ID

Nhà sản xuất phải có khả năng tạo HW_ID theo định đạng được yêu cầu trong Tiêu chuẩn. Giá trị này là ngẫu nhiên sao cho chúng không liên tục và không lặp lại.

Người dùng ứng dụng của Nhà sản xuất không thể xem hoặc trích xuất thông tin HW_ID từ ứng dụng.

10.10.5 Ghi lại HW_ID

Nhà sản xuất phải ghi lại trong một **Sổ đăng ký HW_ID**, các giá trị của mỗiHW_ID được tạo.Chi tiết này được tạo sẵn khi SA yêu cầu.

11. GIẢI THÍCH VÀ MÃ LỖI TRONG S-63

Mã lỗi	Lỗi/Thông điệp cảnh báo
SSE 01	*"Self Signed Key is invalid"*
	"Khóa tự ký không hợp lệ"
SSE 02	*"Format of Self Signed Key file is incorrect"*
	"Định dạng tập tin Khóa tự ký không chính xác"
SSE 03	*"SA Signed Data Server Certificate is invalid"*
	"Chứng chỉ Data Server được SA ký không hợp lệ"
SSE 04	*"Format of SA Signed DS Certificate is incorrect"*
	"Định dạng Chứng chỉ Data Server được SA ký không chính xác"
SSE 05	*"SA Digital Certificate (X509) file is not available. A valid certificate can be obtained from the IHO website or your data supplier"*
	"Không có sẵn tệp Chứng chỉ số SA (X509). Có thể thu về Chứng chỉ hợp lệ từ trang web IHO hoặc nhà phân phối dữ liệu của bạn"
SSE 06	*"The SA Signed Data Server Certificate is invalid. The SA may have issued a new public key or the ENC may originate from another service. A new SA public key can be obtained from the IHO website or from your data supplier"*
	"Chứng chỉ Data Server được SA ký không hợp lệ. SA có thể đã phát hành một khóa chung mới hoặc ENC có thể sinh ra từ một dịch vụ khác. Có thể thu về khóa chung SA từ trang web IHO hoặc từ nhà phân phối dữ liệu"
SSE 07	*"SA signed DS Certificate file is not available. A valid certificate can be obtained from the IHO website or your data supplier"*
	"Không có sẵn tập tin Chứng chỉ Data Server được SA ký. Có thể thu về Chứng chỉ hợp lệ từ trang web IHO hoặc của nhà phân phối dữ liệu"
SSE 08	*SA Digital Certificate (X509) file incorrect format. A valid certificate can be obtained from the IHO website or your data supplier*
	"Định dạng tập tin chứng chỉ số SA (X509) không chính xác. Có thể thu về Chứng chỉ hợp lệ từ trang Web IHO hoặc từ nha phân phối dữ liệu"
SSE 09	*ENC Signature is invalid*
	"Chữ ký ENC không hợp lệ"
SSE 10	*Permits not available for this Data Server. Contact your data supplier to obtain the correct permits.*
	"Không có sẵn giấy phép cho Data Server này. Liên hệ với nhà cung cấp dữ liệu để thu về giấy phép hợp lệ"
SSE 11	*Cell Permit not found. Load the permit file provided by the data supplier.*
	"Không tìm thấy giấy phép. Tải tập tin giấy phép được cung cấp từ nhà phân phối dữ liệu".
SSE 12	*Cell Permit format is incorrect. Contact your data supplier and obtain a new permit file.*
	"Định dạng giấy phép không đúng. Liên hệ với nhà cung cấp dữ liệu và thu về một giấy phép mới"
SSE 13	*Cell Permit is invalid (checksum is incorrect) or the Cell Permit is for a differentsystem". Contact your data supplier and obtain a new or valid permit file.*
	"Giấy phép không hợp lệ (Checksum không chính xác) hoặc giấy phép được sử dụng trên một hệ thống khác. Liên hệ với nhà phân phối dữ liệu để thu về giấy

Mã lỗi	Lỗi/Thông điệp cảnh báo
	phép mới hoặc giấy phép hợp lệ"
SSE 14	*Incorrect system date, check that the computer clock (if accessible) is set correctly or contact your system supplier.*
	"Ngày hệ thống không chính xác, kiểm tra đồng hồ máy tính (nếu có thể) để thiết lập lại cho đúng hoặc liên hệ với nhà cung cấp hệ thống của bạn"
SSE 15	*Subscription service has expired. Please contact your data supplier to renew the subscription licence*
	"Đã hết hạn sử dụng giấy phép. Vui lòng liên hệ với nhà cung cấp dữ liệu của bạn để làm mới giấy phép sử dụng."
SSE 16	*ENC CRC value is incorrect. Contact your data supplier as ENC(s) may be corrupted or missing data.*
	"Giá trị CRC không chính xác. Liên hệ với nhà phân phối dữ liệu vì ENC có thể bị lỗi hoặc thiếu dữ liệu"
SSE 17	*Userpermit is invalid (checksum is incorrect). Check that the correct hardware device (dongle) is connected or contact your system supplier to obtain a valid userpermit.*
	"User Permit không hợp lệ (Check Sum không đúng). Kiểm tra lại thiết bị phần cứng (dongle) đã được kết nối hay chưa hoặc liên hệ với nhà cung cấp hệ thống của bạn để nhận User Permit hợp lệ"
SSE 18	*HW_ID is incorrect format*
	"Định dạng HW_ID không chính xác"
~~**SSE 19**~~	~~*"Permits are not valid for this system. Contact your data supplier to obtain the correct permits"*~~
	~~*"Giấy phép không hợp lệ cho hệ thống này. Liên hệ với nhà cung cấp dữ liệu để thi về Giấy phép hợp lệ"*~~
SSE 20	*Subscription service will expire in less than 30 days. Please contact your data supplier to renew the subscription licence*
	"Giấy phép sẽ hết hạn trong thời gian ít hơn 30 ngày. Vui lòng liên hệ với nhà phân phối dữ liệu để làm mới giấy phép"
SSE 21	*Decryption failed no valid cell permit found. Permits may be for another system or new permits may be required, please contact your supplier to obtain a new licence*
	"Giải mã thất bại do không tìm thấy giấy phép hợp lệ. Giấy phép có thể cho hệ thống khác hoặc giấy phép mới được yêu cầu, vui lòng liên hệ với nhà cung cấp dữ liệu để thu về giấy phép mới"
SSE 22	*SA Digital Certificate (X509) has expired. A new SA public key can be obtained from the IHO website or from your data supplier.*
	"Chứng chỉ số SA (X509) đã hết hạn. Có thể thu về Khóa chung SA mới từ trang Web IHO hoặc từ Nhà phân phối dữ liệu của bạn."
SSE 23	*Non sequential update, previous update(s) missing try reloading from the base media. If the problem persists contact your data supplier.*
	"Thiếu bản cập nhật theo trình tự, thử cài đặt lại từ CD. Nếu vấn đề vẫn còn tiếp diễn, liên hệ với nhà phân phối dữ liệu của bạn"
SSE 24	*ENC Signature format incorrect, contact your data supplier*
	"Định dạng Chữ ký ENC không chính xác, liên hệ với nhà phân phối dữ liệu của bạn"

Mã lỗi	Lỗi/Thông điệp cảnh báo
SSE 25	*Viewer – "The permit for ENC<cell name> has expired. This cell may be out of date and MUST NOT be used for Primary NAVIGATION".*
	Người xem – "Giấy phép cho ENC (Cell Name) đã hết hạn. Cell này đã lỗi thời và KHÔNG ĐƯỢC sử dụng cho mục đích HÀNG HẢI"
SSE 26	*This ENC is not authenticated by the IHO acting as the Scheme Administrator*
	"ENC này chưa được xác nhận bởi IHO (tức là Nhà quản trị Lược đồ)"
SSE 27	*Viewer – "ENC<cell name> is not up to date. A New Edition, Re-issue or Update for this cell is missing and therefore MUST NOT be used for Primary NAVIGATION".*
	Người xem – "ENC <cell name> đã lỗi thời. Thiếu một Phiên bản mới, dữ liệu tái bản hoặc cập nhật, do đó KHÔNG ĐƯỢC sử dụng cho mục đích Hàng Hải.

SSE 01 phải được trả về khi Khóa tự ký (SSK) không được xác nhận dựa vào khóa chung lưu trữ như một phần của SSK. Data Server phải kiểm tra SSK của chính nó là hợp lệ trước khi gửi tới SA.SA sẽ xác nhận SSK của Data Server trước khi trả về Chứng chỉ Data Server được SA ký.

SSE 02 phải được trả về nếu định dạng SSK không đúng. Do các thành phần của SSK hoặc các ký tự bị thiếu. SA và Data Server phải hoàn thành việc kiểm tra này.

SSE 03 phải được trả về nếuChứng chỉ Data Server được SA ký không được xác thực một cách chính xácdựa vào Khóa chung SA. Quá trình xác nhận này phải được thực hiện bởi SA trước khi cung cấp nó cho Data Server.Data Server phải xác nhận chứng chỉ SA nhận được từ SA.Data Client phải xác nhận Chứng chỉ SA chứa trong tập tin Chữ ký ENC trước khi giải mã.

SSE 04 phải được trả về nếu Chứng chỉ Data Server được SA ký có định dạng không đúng.Điều này phải được thực hiện bởi Data Server khi nhận được từ SA.

SSE 05 phải được trả về nếu không có chứng chỉ được cải đặt trên Data Client hoặc đường dẫn tới nó không tìm thấy.

SSE 06 phải được trả về nếu Chứng chỉ số SA (khóa chung) không được dựa vào những điều sau:

Chứng chỉ số SA sẽ không được xác nhận dựa vào Khóa chung SA.

Khóa chung của SA chứa trong Chứng chỉ số sẽ không được xác thực dựa vào chữ ký chứa trong tập tin Chữ ký ENC. Điều này có thể là một trường hợp của Chứng chỉ không có căn cứ hoặc không hợp lệ hoặc định dạng chữ ký không chính xác.

SSE 07 phải được trả về nếu Chứng chỉ Data Server được SA ký không có sẵn cho Data Server kiểm tra hoặc không có mặt trong tập tin Chữ ký ENC khi Data Client cố gắng xác nhận nó.

SSE 08 phải được trả về khi Khóa chung của SA tổ chức trong Chứng chỉ số SA có định dạng không đúng hoặc tập tin Chứng chỉ không đọc được.

SSE 09 phải được trả về nếu thành phần Chữ ký ENC trong tập tin chữ ký

ENC không được xác thực dựa vào Khóa chung của Data Server chứa trong thành phần chứng chỉ của tập tin chữ ký ENC.

SSE 10 phải được trả về nếu không có Cell Permit có sẵn cho Data Server cụ thể phù hợp với Bộ sản phẩm trao đổi được tải lên.

SSE 11 phải được trả về nếu không có giấy phép được cài đặt trên hệ thống.

SSE 12 phải được trả về nếu Cell Permit có định dạng không chính xác.

SSE 13 phải được trả về nếu CRC được tính toán của Cell Permit không được xác nhận dựa vào CRC được tổ chức trong Cell Permit. [Data Client] Điều này có thể do HW_ID có vấn đề, bị lỗi trong quá trình chuyển giao hoặc Giấy phép được dùng cho một hệ thống khác.

SSE 14 phải được trả về nếu ngày hệ thống không đồng nhất với ngày thu được từ bất kỷ giải pháp thay thế, ngày từ nguồn đáng tin cậy, ví dụ như GPS (Data Client).

SSE 15 phải được trả về nếu ngày hết hạn của Cell Permit có kỳ hạn sớm hơn so với ngày thu được từ ngày hệ thống được xác nhận. [Data Client].

SSE 16 phải được trả về nếu giá trị CRC được tính toán của ENC (sau khi giải mã và giải nén) không được xác nhận dựa vào giá trị CRC tương ứng trong tập tin CATALOG.031. Điều này cũng áp dụng cho các tập tin chữ ký, text, hình ảnh không được mã hóa.[Data Client].

SSE 17 phải được trả về nếu CRC chứa trong User Permit không được xác nhận dựa vào CRC tính toán từ HW_ID được trích xuất [Data Server].

SSE 18 phải được trả về nếu HW_ID đã mã hóa được trích xuất từ User Permit có định dạng không chính xác [Data Server].

~~**SSE 19** phải được trả về nếu HW_ID được lưu trữ trong thiết bị phần cứng/phần mềm bảo mật không giải mã Cell Permit được tải lên hoặc đã cài đặt trên hệ thống.~~

SSE 20 phải được trả về nếu Giấy phép hết hạn trong 30 ngày hoặc ít hơn.

SSE 21 phải được trả về nếu Cell Key hợp lệ (khóa giải mã) không thu được từ Cell Permit liên quan cho phép hệ thống giải mã cell ENC tương ứng.

SSE 22 phải được trả về nếu Chứng chỉ số SA (X509) bị hết hạn.Đó là nếu ngày "**hợp lệ để**" trong Chứng chỉ cũ hơn ngày hệ thống được xác nhận.

SSE 23 phải được trả về nếu ENC cập nhật được nhập vào không liên tục với bản cập nhật mới nhất đã chứa trong SENC cho bất cứ Cell được đưa ra. Dưới các điều kiện của quy trình cập nhật (cho mỗi cell) phải kết thúc và ECDIS hiển thị một cảnh báo khi cell được hiển thị là cell đã lỗi thời và không được sử dụng cho hàng hải.

SSE 24 phải được trả về nếu định dạng chữ ký ENC (cặp R và S thứ nhất) không tương thích với định dạng nêu trong tài liệu này.Theo các điều kiện này, quá trình nhập cell sẽ kết thúc nhưng hệ thống sẽ tiếp tục xác nhận tính toàn vẹn của các cell còn lại.

SSE 25 phải được trả về nếu giấy phép sử dụng ENC lưu trữ cho các cell đưa ra đã hết hạn. Các cell có thể xem được nhưng một tin nhắn cảnh báo phải thường xuyên hiển thị cho người sử dụng, ví dụ: "Giấy phép cho ENC <cell name> đã hết hạn. Cell này có thể đã lỗi thời và KHÔNG ĐƯỢC sử dụng cho

mục đích HÀNG HẢI".

SSE 26 phải được trả về nếu Chứng chỉ tự ký (trong tập tin Chữ ký ENC) xác nhận dựa vào một tập tin Chứng chỉ hoặc Khóa chung được lưu trữ trên Data Client khác với chứng chỉ được cung cấp bởi SA. Điều này phục vụ cho trường hợp có nhiều Chứng chỉ hoặc Khóa chung được lưu trữ trong Data Client.

SSE 27 phải được trả về nếu trạng thái của cell bịxem như không cập nhật đối với tập tin PRODUCTS.TXT mới nhất được tải lên hoặc duy trì trên hệ thống. Một thông điệp cảnh báo phải thường xuyên được hiển thị trên màn hình thông tin cho người dùng như *: "ENC <cell name>đã lỗi thời. Có thể thiếu Phiên bản mới, Dữ liệu tái bản hoặc cập nhật cho cell này và do đó KHÔNG ĐƯỢC sử dụng cho mục đích HÀNG HẢI"*.

S-63 Phụ lục A.
Thủ tục yêu cầu Chứng chỉ Data Server

1 Mục đích

Mục đích của thủ tục này là để xác định quy trình để Data Server thu về Chứng chỉ Data Server được SA ký từ SA như được định nghĩa trong Tiêu chuẩn S-63 - Lược đồ Bảo vệ Dữ liệu.

2 Trách nhiệm

2.1 Sự cần thiết của Chứng chỉ Data Server

Một tổ chức mã hóa và ký chữ ký số lên dữ liệu ENC là một phần của Lược đồ Bảo vệ dữ liệu S-63 sẽ yêu cầu Chứng Chỉ Data Server được ký bởi SA.

Người dùng dữ liệu ENC đã mã hóa và được ký chữ ký số (ví dụ hệ thống ECDIS xác thực chữ ký và giải mã thông tin ENC) không cần Chứng chỉ Data Server.Các đại lý hoặc nhà phân phối dữ liệu sẽ chỉ cung cấp dịch vụ ENC được cung cấp bởi Data Server không yêu cầu Chứng chỉ Data Server.

2.2 Cơ quan Thủy đạc và Tổ chức RENC

Tất cả các cơ quan thủy đạcvà tổ chức RENC (Trung tâm phối hợp vùng ENC) chỉ phải hoàn thành Phần I của mẫu đơn kèm theo, bao gồm các thông tin cần thiết đểxin một Chứng chỉ Data Server. Một Data Server chỉ có thể thu về một Chứng chỉ Data Server.

2.3 Không phải Cơ quan Thủy đạc và tổ chức RENC

Các tổ chức thương mại khác mong muốn hoạt động như Data Server để mã hóa và ký chữ ký số lên thông tin ENC tuân theo Lược đồ bảo vệ cũng có thể xin một Chứng chỉ Data Server. Tuy nhiên, các tổ chức này phải được một Data Server đã là thành viên của Lược đồ bảo vệ tán thành yêu cầu và hoàn thành Phần II của mẫu đơn đính kèm. Data Server cung cấp dữ liệu ENC để các tổ chức thương mại đồng ý yêu cầu.

2.4 Cục Thủy đạc Quốc tế(IHB)

IHB như là một Nhà quản trị Lược đồ có trách nhiệm tạo chứng chỉ Data Server phù hợp với thủ tục nội bộ.

3 Các định nghĩa

Data Server: Đây là thuật ngữ được sử đụng dể xác định một tổ chức tạo ra dữ liệu ENC đã mã hóa được ký chữ ký số và phát hành Cell Permit tới Data Clients (người dùng cuối cùng).

Chứng chỉ : (Certificate) Chứng chỉ là tài liệu dạng số xác nhận sự ràng buộc của khóa chung tới một tổ chức hoặc cá nhân. Chứng chỉ đểxác minh rằng một khóa chung cụ thể thuộc một tổ chức cụ thể, trong trường hợp này là IHO.

3.1 Tham khảo

[1] Lược đồ bảo vệ dữ liệu IHO – S-63, IHO

[2] S-57 - Tiêu chuẩn chuyển đổi cho Dữ liệu thủy đạc dạng số, IHO.

4 Thủ tục

Chương này định nghĩa luồng thông tin, trách nhiệm và hướng dẫn chi tiết các công việc.

4.1 Hoàn thành mẫu đơn đính kèm

Một Data Server đã được Cơ quan Thủy đạc hoặc tổ chức RENC công nhận, mong muốn tham gia vào Lược đồ Bảo mật dữ liệu hải đồ điện tử(S-63), chịu trách nhiệm cung cấp các thông tin sau đây tới IHO:

- Thỏa thuận Data Server được IHO ký.
- Mẫu đơn chứng chỉ,yêu cầu điền đủ thông tin Phần 1, đã được ký.
- Khóa chung của Data Server
- Chứng chỉ tự ký (SSK) của Data Server

4.2 Nhu cầu xác nhận

Tất cả các tổ chức không phải là cơ quan thủy đạc và RENC mong muốn trở thành một Data Server phải có Mẫu đơn chứng chỉ yêu cầu (Certificate Request Form) được xác nhận bởi một Data Server hiện đang là thành viên của Lược đồ.

4.3 Công nhận tổ chức

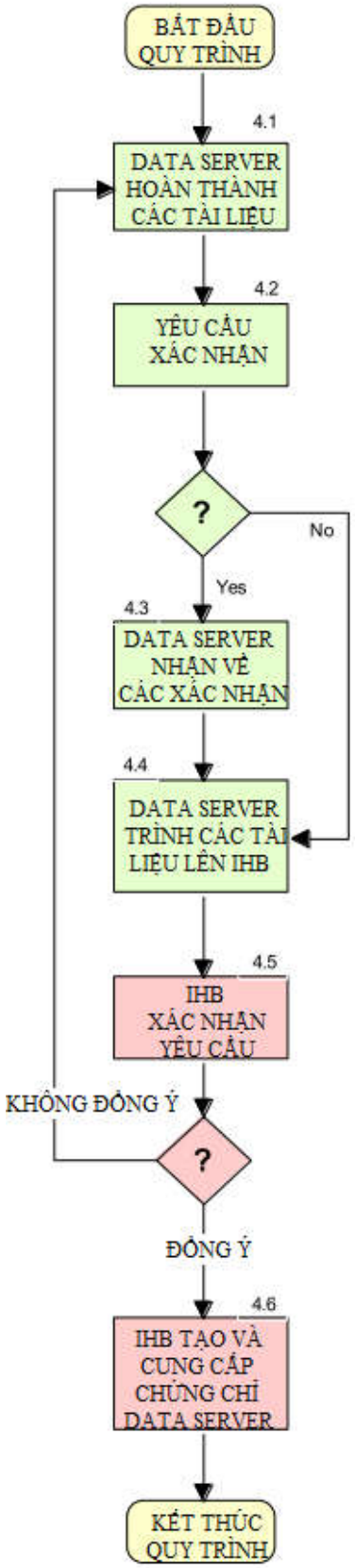
Việc công nhận Data Server phải hoàn thành Phần II Mẫu đơn chứng chỉ yêu cầu và nộp lại cho cơ quan không phải là Cơ quan Thủy đạc hoặc RENC.

4.4 Nộp yêu cầu tới IHO

Data Server chịu trách nhiệm nộp Đơn yêu cầu đã đã hoàn tất cùng với tất cả các thông tin khác được liệt kê trong phần 4.1 ở trên tới IHB.

4.5 Xác nhận Chứng chỉ yêu cầu

IHB sẽ xác nhận nguồn gốc của Chứng chỉ yêu cầu và xác thực khóa chung bằng cách liên hệ tới Data Server. Họ cũng sẽ đảm bảo nhu cầu cho Chứng chỉ Data Server có hiệu lực bằng cách liên hệ với Data Server để xác nhận.IHB sẽ báo các lỗi sai lại cho người đăng ký.



4.6 Tạo Chứng chỉ Data Server

IHB chịu trách nhiệm xác thực SSK được tạo bởi Data Server. Nếu đáng tin thì IHB sau đó sẽ ký lên Khóa chung của Data Server để tạo Chứng chỉ Data Server, sau đó cung cấp tới các Data Server.

5 Các tiêu chuẩn chất lượng

IHB lưu trữ thông tin Data Server yêu cầu và tập tin đính kèm phù hợp với các thủ tục nội bộ.

IHO S-63 Data Protection Scheme
Data Server Certificate Request Form

Ed.1-2003

Form to be returned to:
International Hydrographic Bureau
4, Quai Antoine 1er+, 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 Data Server organisation
Organisation:.....
Address: .....
Address: .....
Address: .....
Postalnumber/place:.....**Country**: .....
Tel: .....**Fax**: .....**Web**: .....
Administrativepointofcontact: **Technicalpointofcontact**:
Name:.....**Name**: .....
Tel: .....**Tel**: .....
E-mail: ..... **E-mail**: .....
Please verify the following information is included:
□ All fields in Part 1 & 2 of this form are completed
□ Data Server Public Key
□ Data Server Self Signed Key (SSK)
□ Signed IHO S-63 Data Server Agreement, or □ already available with IHB

Signeddate: .....**Name**: .....
Part II: To be completed by endorsing HO or RENC organisation
Organisation: .....
Contact name:.....
Tel: .....**Fax**: .....**E-mail**:.....
Part III: To be completed by IHB
□ Form and attachments validated
□ Signed Data Server Agreement, ref. ……..
□ Certificate created date: ..... File ref:.....
□ Certificate returned to Data Server
Signed date: .....**Name**: .....

S-63 Phục lục B
Thủ tục yêu cầu thông tin Nhà sản xuất ECDIS

1 Mục đích

Mục đích của thủ tục này là để xác định quy trình một OEM có thể thực hiện để trở thành một bên tham gia Lược đồ Bảo mật dữ liệu hải đồ điện tử(S-63).Để tham gia, các OEM sẽ yêu cầu giá trị M_ID và M_KEY cho chính họ.Đây là các giá trị được cung cấp bởi SA được định nghĩa bởi Lược đồ bảo vệ dữ liệu sao cho OEM có thể giải mã dữ liệu ENC đã mã hóa S-63.

2 Trách nhiệm

2.1 OEM

OEM phát triển ứng dụng Data Clientcần giá trị M_ID và M_KEYduy nhất.IHB (là Nhà quản trị lược đồ) sẽ chia sẻ thông tin này với tất cả Data Server tham gia Lược đồ.Một OEM chỉ được cấp một cặp M_ID và M_KEY.

Giá trị M_ID và M_Key sẽ được trả lạiSA nếu tổ chức ngừng giao dịch hoặc không còn hỗ trợ ứng dụng truy cập và hiển thị dữ liệu ENC đã mã hóa S-63.Data Server sẽ được thông báo về các trường hợp như vậy sao cho không có giấy phép mới được phát hành cho hệ thống nhà sản xuất ECDIS riêng biệt.

Không cần phải cho Data Client quyền truy cập tới giá trị M_KEY bởi vì nó được xây dựng một cách bảo mật trong ứng dụng người dùng cuối cùng (ví dụ Dongle) và được cung cấp tới Data Client ở dạng đã mã hóa, được biết đến như một User Permit.

2.2 Cục Thủy đạc Quốc tế

IHB (như là một SA) có trách nhiệm duy nhất là tạo ra giá trị M_ID và M_KEY và cung cấp chúng tới OEM và phân phối giữa các Data Server.

3 Định nghĩa

M_ID:	Mã định danh nhà sản xuất ECDIS
M_KEY:	Khóa nhà sản xuất ECDIS
OEM:	Nhà sản xuất thiết bị ECDIS
User Permit:	Một chuỗi 28 ký tự chữ-số chứa HW_ID được mã hóa của Data Client với M_KEY của Nhà sản xuất ECDIS và chứa M_ID.
Dongle:	Thiết bị khóa cứng chứa HW_ID của hệ thống Data Client

3.1 Tham khảo

[1] Lược đồ bảo vệ dữ liệu IHO S-63, IHO

[2] S-57 Tiêu chuẩn chuyển đổi dữ liệu thủy đạc dạng số, IHO

4 Thủ tục

Chương này xác định luồng thông tin, trách nhiệm và hướng dẫn chi tiếtcông việc.

4.1 Hoàn thành Mẫu đơn yêu cầu

OEM chịu trách nhiệm hoàn thành tất cả các thông tin trong Phần 1 của mẫu đơn yêu cầu M_ID và M_KEY được đính kèm. IHO có thể muốn yêu cầu cung cấp thêm tài liệu như là Thỏa thuận bảo mật – việc này chưa được miêu tả chi tiết tại đây

Lưu ý rằng một OEM có thể:

- Chỉ được chỉ định một cặp M_ID và M_KEY
- Phải trả lại thông tin cho SA nếu dừng giao dịch hoặc không cung cấp sản phẩm xác thực chữ ký hoặc không còn có nhu cầu giải mã thông tin ENC.

4.2Xác minh Mẫu đơn yêu cầu

SA xác minhtất cả thông tin trong Phần I của Đơn yêu cầu đã hoàn thành, hoặc cung cấp thông tin cho OEM về các thông tin bị thiếu.

4.3 Xác minh Thỏa thuận bảo mật đã ký

SA xác minh rằng một Thỏa thuận bảo mậtđã ký đã được bao gồm với yêu cầu hoặc sẵn có trong kho lưu trữ IHB.Nếu Thỏa thuận không có sẵn, thông báo tới OEM về các yêu cầu bắt buộc cho một Thỏa thuận đã ký.

4.4 Xác nhận kiểm tra thành công Dữ liệu kiểm tra S-63.

Xác minh rằng OEM đã hoàn thành toàn bộ việc kiểm tra của ứng dụng với dữ liệu kiểm tra IHO S-63 có sẵn.Nếu không, yêu cầu OEM xác định hoàn tất các thủ tục kiểm tra trước khi M_ID và M_KEY được cung cấp.

4.5 Kiểm tra OEM hiện không có M_ID và M_KEY

Xác minh OEM không có M_ID và M_KEY được chỉ địnhtrước đó.Nếu không, thông báo cho OEM về vấn đề này.

4.6 Tạo M_ID và M_KEY

SA gán cho OEM một tổ hợp M_ID và M_KEY sẵn có và duy nhất.

4.7 Thông báo về M_ID và M_KEY mới

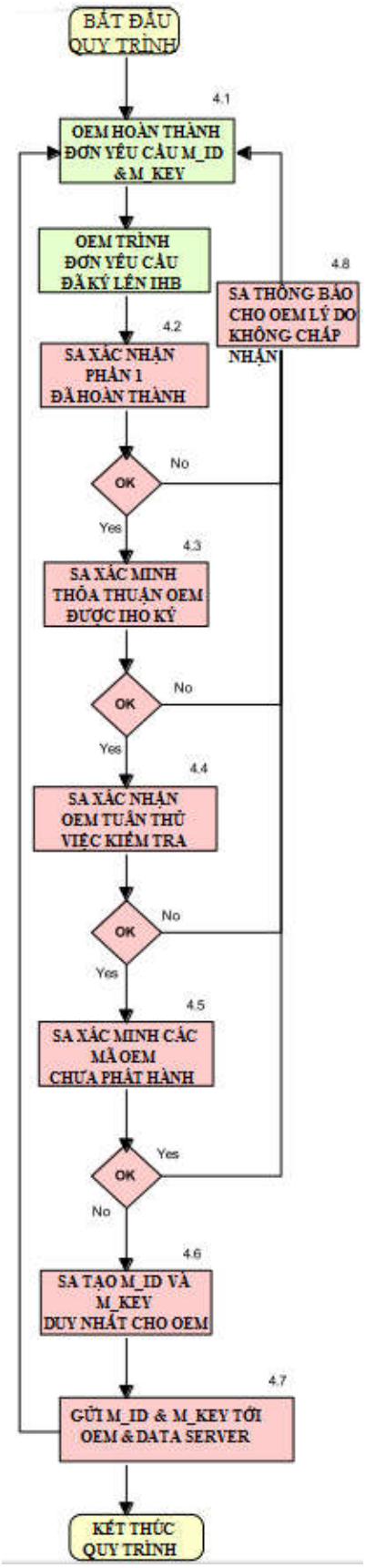
SA thông báo tới OEM về M_ID và M_KEY của họ.SA thông báo tới tất cả các Data Server đã đăng ký về thông tin M_ID và M_KEY mới.

4.8 Thông báo cho OEM các vấn đề với Đơn yêu cầu

SA thông báo cho OEM về các vấn đề cụ thể với các yêu cầu và yêu cầu cập nhật thông tin để được cung cấp trước một M_ID và M_KEY có thể được chỉ định. Tiếp tục quá trình xử lý yêu cầu bị chấm dứt.

5 Các tiêu chuẩn chất lượng

IHB lưu trữ Đơn yêu cầu và tất cả các thông tin liên quan với thủ tục nội bộ.



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 1er+, 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 Data Server organisation

Organisation:.....
Address: .....
Address: .....
Address: .....
Postalnumber/place: .....**Country**: .....
Tel: .....**Fax**: .....**Web**: .....

Administrativepointofcontact:	**Technicalpointofcontact**:
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 OEM 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

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

Part II: To be completed by IHB

☐Verify Part 1 is completed
☐Signed OEM Agreement available, ref. .....
☐ Verify OEM does not have a previously issued M_ID and M_KEY
☐Assigned M_ID: ..... M_KEY: .....
☐M_ID and M_KEY returned to OEM and all registered Data Servers
Signed date: .....**Name**: .....

S-63 Phụ lục 1 [Bộ dữ liệu kiểm tra S-63]
Dữ liệu kiểm tra cho Lược đồ Bảo mật dữ liệu hải đồ điện tử(S-63)

Lưu ý quan trọng: S-63 phụ lục 1 bao gồm dữ liệu kiểm tra được cung cấp riêng rẽ như tập tin được nén (ZIP) (xem mục S-63 trên trang web IHO). Bên trong tập tin ZIP này là một tài liệu "Hướng dẫn thực hiện kiểm tra dữ liệu" để hướng dẫn sử dụng dữ liệu kiểm tra.Các văn bản dưới đâytrình bày ngắn gọn về Phụ lục 1.

1 Giới thiệu

S-63 Phụ lục 1xác định các khuyến nghị về định nghĩa kiểm tra và dữ liệu kiểm tra của các nhà phát triển ứng dụng cho Data Server và Data Client hiểu cấu trúc an ninh được định nghĩa trong S-63 và kiểm tra xem ứng dụng của họ có phù hợp với tiêu chuẩn. Nó bao gồm một "Hướng dẫn thực hiện kiểm tra dữ liệu" được cung cấp cùng với Dữ liệu kiểm tra.

S-63 Phụ lục 1 được duy trì bởi IHO DPSWG.Nhiều dữ liệu kiểm tra có thể được đưa ra trong tương lai dựa trên thông tin phản hồi từ người dùng để cung cấp nền tảng kiểm tra đầy đủnhằm xác minh tính đúng đắn và tuân thủ tiêu chuẩn hoặc để ứng dụng người dùng cuối cùng nhận biết các tình huốngsai phạm. Phiên bản hiện tại của tài liệu cung cấp toàn bộ mẫu kiểm tra để kiểm tra việc tuân thủ.

Tài liệu "Hướng dẫn thực hiện kiểm tra dữ liệu" sẽ được duy trì độc lập với tài liệu chínhcủa IHO S-63 và phiên bản mới sẽ được công bố trên trang web IHO.

2 Tổ chức của Định nghĩa kiểm tra và dữ liệu kiểm tra

2.1 Định nghĩa kiểm tra

Định nghĩa kiểm tra cung cấp các hàm kiểm tra mức độ cao được khuyếncáo để kiểm tra sự tuân thủ cấu trúc bảo mật theo định nghĩa trong S-63. Nó không thay thế đơn vị kiểm tra trong phát triển phần mềm nhưng đưa ra cấu trúc đầu vào cho các chức năng kiểm tra phần mềm.

Định nghĩa kiểm tra được tổ chức trong chức năng và quy định trong chương 3 của tài liệu "Hướng dẫn thực hiện kiểm tra dữ liệu".Định nghĩa kiểm tra cho chức năng Nhà quản trị lược đồkhông bao gồm trong tài liệu vì chỉ IHB sẽ yêu cầu các kịch bản kiểm tra này.

Mỗi định nghĩa kiểm tra: kiểm tra các ứng dụng của Data Server hoặc Data Client.Lưu ý rằng quá trình kiểm tra liên quan tới tất cả ứng dụng nếu loại ứng dụng được bỏ qua.

Có định nghĩa kiểm tra cho cả điều kiện kiểm tra đúng và điều kiện kiểm tra sai để đảm bảo một ứng dụng mạnh và phản ánh điều kiện hoạt động.

Lưu ý rằng IEC sẽ chịu trách nhiệm xác định loại ECDIS thích hợpđồng ý sự kiểm tra bổ sung trong tài liệu này.

2.2 Dữ liệu kiểm tra

Một dãy dữ liệu kiểm tra được phát triển để hỗ trợ định nghĩa kiểm tra.Đặc điểm từng Bộ dữ liệu kiểm tra được định nghĩa trong chương 4 của tài liệu "Hướng dẫn thực hiện kiểm tra dữ liệu".

Một loạt các dữ liệu kiểm tra được tổ chức trong tập tin ZIP và sẽ giải nén vào một cấu trúc thư mục nơi mỗi dữ liệu kiểm tra được đặt trong một thư mục riêng biệt. Lưu ý rằng một số bộ dữ liệu kiểm tra được dùng trong nhiều định nghĩa kiểm tra.

Lưu ý rằng Dữ liệu kiểm tra cũng có thể được sử dụng bởi các nhà phát triển để kiểm tra đơn vị hoặc kiểm tra tình huống khác cho ứng dụng của họ.

2.3 Điều kiện sử dụng dữ liệu kiểm tra

Thông tin ENC (cần thiết) bao gồm trong dữ liệu kiểm tra đã được tạo sẵn cho người nhận để kiểm tra ứng dụng của họ và xác minh sự tuân thủ tiêu chuẩn S-63.Các tài liệu được cung cấp theo các điều kiện bên dưới. Nếu người nhận không đồng ý bị ràng buộc bởi các điều kiện này thì các thông tin ENC không nên được sử dụng và nó sẽ bị hủy.

2.3.1 Điều kiện phát hành

Tài liệu quan trọng được bảo vệ bởi bản quyền của Cơ quan thủy đạc quốc gia. Không bộ phận nào của tài liệu cung cấp được tái bản, lưu trữ trong một hệ thống phục hồi hoặc lan truyền dưới mọi hình thức hoặc bằng bất kỳ phương tiện nào, điện tử, cơ học, sao chụp hoặc trừ khi cần thiết để thực hiện các mục đích mô tả ở trên.

Tài liệu KHÔNG được sử dụng cho mục đích hàng hải.

Khi tài liệu không còn cần thiết để thực hiện mục đích này, nó và bất cứ bản sao làm việc phải bị tiêu hủy.

2.3.2 Miễn trừ trách nhiệm

Trong khi IHB và Cơ quan thủy đạc nỗ lực để đảm bảo rằng tài liệu phù hợp để thực hiện các mục đích, họ không đưa ra giấy bảo hành hoặc sự bảo đảm khác vì mục đích đó, mà nó sẽ đáp ứng được các yêu cầu. IHB và Cơ quan thủy đạc sẽ không chịu trách nhiệm cho các thiệt hại hoặc mất máttrong quá trình. Tài liệu cung cấp được sử dụng thuộc trách nhiệm của người nhận.

S-63 Phụ lục 2 [Large edia Support]

1 Giới thiệu

Cho đến gần đây đa số ECDIS/ECS chỉ có khả năng tải Bộ Sản phẩm trao đổi ENC (ExSets) từ CD-ROM. Tuy nhiên, điều nàyngày càng trở nên phổ biến với phần cứngOEM mới để cung cấp đĩa DVD hoặc phương tiện hỗ trợ lớn[16] (Large Media Support- LMS). Việc đưa vào phương tiện hỗ trợ này cung cấp cho Data Server khả năng gồm nhiều dữ liệu ENC trên một đĩa DVD đơn.

Một số vấn đề nảy sinh trong quá trình hoạt động của Dịch vụ ENC mã hóa S-63 bằng cách sử dụng ấn bản 1.0 của tiêu chuẩn.Phần lớn vấn đề này là việc cung cấp Bộ sản phẩm trao đổi lớn dẫn đến thời gian tải lên ECDIS/ECS chậm. Đây là một trong những lý do chính khiến Data Server không cung cấp dịch vụ gồm các Bộ sản phẩm trao đổi đơn lẻmà mở rộng ra nhiều CD-ROM.

Việc lưu trữ một Bộ Sản phẩm trao đổi ENC duy nhất trên một thiết bị lưu trữ như DVD hoặc USB có kích thước tương đương CD-EOM, sẽ sử dụng không hiệu quả CD và bộ nhớ sẵn có. Nên lưu trữ nhiều Bộ sản phẩm trao đổi trên cùng phương tiện, mỗi kích cỡ tương tự như vậy hiện lưu trữ trên CD-ROM. Vì phương pháp lưu trữ này không được định nghĩa trong IHO S-57 -Chi tiết kỹ thuật sản phẩm hoặc Ấn bản 1.0 của S-63 một cấu hình mới phải được xác định.

Khi thiết kế cấu trúc media thì cần xem xét tính đến những điều sau:

- Dịch vụ ENC có thể được cung cấp qua nhiều bộ media
- Dịch vụ ENC có thể chứa dữ liều từ nhiều Data Server
- Tập tin thích hợp phải được cung cấp sao cho Hệ thống nhà sản xuất ECDIS có thể quản lý và nhập vào dữ liệu ENC được mã hóa S-63 một cách hiệu quả và nhanh chóng và tạo ra các hệ thống trực quan, quản lý nhiều phần của media dễ dàng.

2 Tổng quan Media

Phần dưới đây đưa ra cách thứcdữ liệu được tổ chức trên Media.Nó cũng vạch ra cấu trúc Bộ sản phẩm trao đổi S-63 được sửa đổi cho DVD. Điều này được hỗ trợ bởi lược đồ trong Phụ chương A và B của phụ lục này. Thông tin chi tiết liên quan đến nội dung và định dạng của tập tin và thư mục này được cung cấp thêm trong phụ lục này.

2.1 Các loại Media

Sẽ có 2 loại media, "**BASE**" chứa một hoặc nhiều Bộ Sản phẩm trao đổi cơ sở và "**UPDATE**" chứa dữ liệu ENC cập nhật hàng tuần, có thể chứa trong một hoặc nhiều Bộ sản phẩm trao đổi trên CD-Update. Nó được coi là do khả năng tăng dung lượng mà cácloại media này cung cấp có thể phát hành lại Bộ sản phẩm trao đổi cơ sở trên CD-Update và ngược lại cung cấp các bản cập nhật hàng tuần trên Base-CD.

2.2 Cấu trúc tập tin và thư mục trên Media

Tất cả Bộ sản phẩm trao đổi đều nằm trong thư mục gốc của mỗi CD bên trong danh mục con cụ thể của riêng chúng. Cấu hình các Bộ sản phẩm trao đổi đều giống nhau như được nêu trong phần 7.5.1 của tài liệu chính với một trường

[16]Large Media Support có thể cũng được biết như là Mass Storage Devices.

hợp ngoại lệ đáng chú ý. Thư mục "**INFO**" bao gồm cả tập tin "**PRODUCTS.TXT**" sẽ không còn được lưu trữ trong thư mục gốc của Bộ sản phẩm trao đổi nhưng lưu trữ trong thư mục gốc của CD.

Thư mục "**INFO**" sẽ tiếp tục được sử dụng bởi Data Server bao gồm tập tin bổ sung duy nhất và cụ thể tới dịch vụ mã hóa ENC theo S-63 của họ. Lưu ý rằng các tập tin của Data Server được lưu trữ trong thư mục này phải đặt tên theo cách mà **KHÔNG LÀM** xung đột với quy ước tên tập tin trong S-63.

2.2.1Bổ sung tập tin Media

Một tập tin bổ sung có tên **"MEDIA.TXT"** được đưa vào trong mỗi phần của Media đểhỗ trợ Data client trong việc quản lý nhiều Bộ sản phẩm trao đổi trên cùng Media và trên nhiều bộ media. Nó cho phép hệ thống Data Client nhắc nhở người dùng chèn media thích hợp bằng cáchthêm vào một thiết bị có thể đọc các chuỗi trong mỗi bản ghi trong từng phần của media. Thông tin chi tiết hơn về định dạng tập tin MEDIA.TXT được cung cấp trong phần 3.

2.3 Nhận diện media

Phải có phương pháp để phân biệt giữa dịch vụ cung cấp trên CD và dịch vụ cung cấp sử dụng *large media support.* Dấu hiệu nhận biết đầu tiên là ID khối của media (xem phần 2.3.1). Điều này sẽ xác định việc sử dụng định dạng *large media* và thông báo cho Data Client về thưmục và cấu trúc tập tin.

Một dấu hiệu nữa là sự có mặt của tập tin MEDIA.TXT mới nằm trong thư mục gốc của Media, theo đó một dịch vụ ENC đang được cung cấp bằng cách sử dụng *large media support.*

2.3.1 Dán nhãn cho Media

Quy ước dán nhãn cho *large media support* giống như được sử dụng trong IHO S-57 - Chi tiết kỹ thuật sản phẩm. Thay vì "V01X01", ở đây, "V" là viết tắt cho "Volume", "M" là viết tắt cho "Media" sẽ được thay thế.

Nhãn các khối của *large media support*cũng chỉ ra có bao nhiêu bộ media trong dịch vụ. Vì vậy, nếu có 3 bộ media thì chúng sẽ được dán nhãn như sau:

M01X03 [Media set 1 of 3]
M02X03 [Media set 2 of 3]
M03X03 [Media set 3 of 3]

LƯU Ý:Điều này chỉ nhận biết số các bộ media trong một dịch vụ ENC và không ám chỉ rằng đây là một Bộ sản phẩm trao đổi đơn nhất bao gồm nhiều bộ media. Mục đích của quy ước đặt tên này là để giúp Data Client nhận biết media (nơi chứa các cell ENC đã đăng ký).

3 Định dạng tập tin Media

3.1 Danh sách sản phẩm (PRODUCTS.TXT)

Tập tin "**PRODUCTS.TXT**" của "**Base Media**" chứa bản ghi tất cả các cell tổ chức trên CD riêng biệt.Phần tiêu đề được định nghĩa như trong phần 6.2.2 của tài liệu chính sẽ được dán nhãn ***"FULL"*** nếu chỉ có một media trong một dịch vụ riêng biệt.Tuy nhiên nếu có nhiều media thì sẽ được dán nhãn là ***"PARTIAL".***Danh sách sản phẩm được dán nhãn "**FULL**" sẽ được cung cấp trên "**UpdateMedia**" với bản ghi của tất cả các cell trong Dịch vụ của Data Server.

Điều quan trọng là các nhà sản xuất ECDIS/ECS phải quản lý các bản ghi

này cẩn thận; Danh sách sản phẩm "**PARTIAL"**phải được sát nhập với danh sách sản phẩm "**FULL"** được lưu trữ trong hệ thống. Phải lưu ý rằng, hệ thống có thể chứa thông tin sản phẩm từ nhiều Data Server. Bởi vậy, điều quan trọng nhất là không ghi đè danh sách "**FULL**" trừ khi chúng được lưu trữ độc lập theo Data Server.

3.2 Danh sách Media (MEDIA.TXT)

Đây là một tập tin mới được thiết kế để quản lý các dịch vụ được cung cấp bằng cách sử dụng *large media support.*Nó nằm trong thư mục gốc của Base CD và Update CD và chứa thông tin liên quan đến tất cả CD trong một dịch vụ của Data Server và các Bộ sản phẩm trao đổi chứa trên CD. Mục đích chính của tập tin này là:

- Cung cấp cho Data Client phương pháp để quản lý nhập vào một dịch vụ của Data Server hỗ trợ *large media.*
- Cung cấp thông tin cho phép Data Client quản lý nhiều bộ media.
- Cung cấp "thông tin người dùng" sao cho Data Client có thể làm cho quá trình nhập vào trực quan hơn tới người dùng cuối cùng.

LƯU Ý: Update CD mới nhất sẽ luôn chứa trạng thái hiện tại của hầu hết các Base CD gần đây nhất (STATUS.LST) và các Bộ sản phẩm trao đổi Base (MEDIA.TXT) trong một dịch vụ của Data Server. Điều này có thể được sử dụng để kiểm tra Base CD và Bộ Sản phẩm trao đổi Base mới nhất đã được cài đặt. Thông tin thêm về cấu trúc và định dạng của tập tin này được tóm lược bên dưới.

3.2.1 Định dạng tiêu đề (Header)

Mục đích của tiêu đề MEDIA.TXT giống như tập tin SERIAL.ENC được lưu trữ cùng với Bộ sản phẩm trao đổi.Nó được sử dụng để quản lý cài đặt CD bằng cách xác địnhnhững nội dung sau:

- Nhà cung cấp dịch vụ CD.
- Ngày và tuần phát hành CD.
- Số và loại CD.
- Máy đọc được tên CD để hiển thị cho người dùng.

Phần tiêu đề được cung cấp trong hai dòng, mỗi dòng chứa một bản ghi riêng, dòng đầu tiên có độ dài cố định và dòng thứ hai được tách biệt bởi dấu phẩy (","). Bảng sau đây xác định định dạng chi tiết hơn:

Trường ID	Vùng định nghĩa	Số Byte	Range
Data Server ID	Ký tự	2	Cặp chữ-số**, ví dụ: PR**
Tuần phát hành	Ký tự	10	Ký tự ASCII, ví dụ **WKNN_YY**
Ngày phát hành	Ngày	8	**YYYYMMDD**
Loại CD	Ký tự	10	Base hoặc Update
Nhãn ID của CD	Ký tự	6	M[01-99]X[01-99]
Dấu hiệu kết thúc bản ghi	Ký tự Hex	2	CR/LF
ID của CD	Ký tự	2-3	Ví dụ M1, M2 hoặc M11

Tên CD đọc được bằng máy	'ký tự'	0-100	Chuỗi text chứa trong dấu ngoặc kép ("")
Thông tin vùng (tùy chọn)	'ký tự'	0-100	Chuỗi text chứa trong dấu ngoặc kép ("")
Dấu hiệu kết thúc bản ghi	Ký tự Hex	2	CR/LF

Ví dụ:

GBWK27_7 20070621 M01X03

M1, 'UKHO Week 27_7 BASE MEDIA 1', 'Europe, Africa, and Middle East'

3.2.2 Định dạng bản ghi Media

Tập tin "MEDIA.TXT" chứa một danh sách bản ghi xác định tất cả các Bộ sản phẩm trao đổi hiện có trong dịch vụ Data Server và đích đến của media, nơi chúng được lưu trữ. Mục đích của tập tin "MEDIA.TXT", cùng với STATUS.LST là cung cấp cho Data Client một phương tiện quản lý đầu vào các ENC đã mã hóa trên nhiều bộ CD và cung cấp "Thông tin người dùng" để Data Client có thể nhắc nhở, bằng cách sử dụng tập tin STATUS.LST, người dùng cuối cùng để tải lên CD thích hợp.

Tập tin "MEDIA.TXT" được lưu trữ trên **UPDATE CD**luôn chứa một danh sách **ĐẦY ĐỦ**của CD/Bộ sản phẩm trao đổi chứa trong dịch vụ Data Server. Nó kèm theo ngày mà Bộ sản phẩm trao đổi phát hành mới, bằng cách này, ECDIS/ECS có thể xác nhận cùng với STATUS.LST cho dù nó có giữ thông tin mới nhất.

Tập tin "MEDIA.TXT" được lưu trữ trên **BASE CD** chứa một danh sách các Bộ sản phẩm trao đổi được lưu trữ trên CD đó.Nó sẽ **KHÔNG**chứa thông tin về các khối khác trong dịch vụ.

Trường ID	Vùng định nghĩa	Số byte	Range	Lưu ý (xem bên dưới)
Vị trí Media/Bộ sản phẩm trao đổi	Ký tự	5-7	**M1** tới **M99**; **B1** tới **B99**. Ví dụ: **M2**; **B7** [Media 2, Base ExS7) **M1** to **M99**;**U1** to **U99** e.g. **M1**;**U2** [Media 1, Update ExS 2]	1
Ngày phát hành Bộ sản phẩm trao đổi	Ngày	8	**YYYYMMDD,** ví dụ: 20070621	2
Số Bộ Media [long Name]	Ký tự		'bất kỳ ký tự ASCII'	3
Thông tin vùng [tùy chọn]	Ký tự		'bất kỳ ký tự ASCII'	4
Trường bảo lưu	Ký tự			5
Trường chú giải	Ký tự			6

Ví dụ:

M1; B1, 20070621, 'Base Dataset 1', 'Europe', ,

Lưu ý:

1. Trường này xác định trên Media vị trí Bộ sản phẩm trao đổi base hay Update.
2. Ngày phát hành ExSet. Đây là ngày mà một ExSet được phát hành hoặc phát hành lại[17] trên Base CD hoặc Update CD. Mặc dù nó có thể thiết thực hơn để phát hành lại tất cả ExSet trên một CD riêng biệt hoặc khi CD được phát hành lại cùng với chỉ một ExSet phát hành lại. Data Client sửdụng ngày này để xác nhận tình trạng của các cell được cài đặt từ Update CD.
3. Một thiết bị đọc được chuỗi văn bản của Data Client để nhắc nhở người dùng cuối tải các media thích hợp.
4. Một thiết bị tùy chọn đọc được chuỗi văn bản được sử dụng bởi Data Client để hiển thị thêm thông tin liên quan tới một khu vực/nhà sản xuất quốc gia trên 1 CD đặc biệt.
5. Ứng dụng trong tương lai.
6. Thông tin chú thích thêm.

Tập tin "MEDIA.TXT" trên Update CD luôn chứa ngày phát hành mới nhất và thông tin cho tất cả các Bộ sản phẩm trao đổi trên Base CD trong một bộ CD.*Mặc dù việccung cấp được thực hiện để có nhiều hơn 1 Bộ sản phẩm trao đổi Update trên Update CD, nó có thể không đầy đủ thông tin như trong phần 4. Tuy nhiên, nếu có nhiều hơn 1 thì có thể được quản lý bởi các mục trong tập tin PRODUCTS.TXT và MEDIS.TXT trên Update CD.*

Ví dụ về một **MEDIA.TXT[UPDATE]** đầy đủ

```
GBWK28_07   20070628UPDATE    M01X02
U1,'UKHO Week 28_07 UPDATE MEDIA 1 of 2','Europe'
M1;B1,20070614,'UKHO BASE MEDIA 1','Europe, Africa and Middle East',,
M1;B2,20070614,'UKHO BASE MEDIA 1','Europe, Africa and Middle East',,
M1;B3,20070621,'UKHO BASE MEDIA 1','Europe, Africa and Middle East',,
M2;B4,20070517,'UKHO BASE MEDIA 2','North and South America',,
M2;B5,20070517,'UKHO BASE MEDIA 2','Morth and South America',,
M3;B6,20070405,'UKHO BASE MEDIA 3','Far East and Australasia',,
M3;B7,20070405,'UKHO BASE MEDIA 3','Far East and Australasia',,
M1;U1,20070628,'UKHO WK28_07 ENC Update','Europe',,
M1;U2,20070628,'UKHO WK28_07 ENC Update','Rest of the World',,
```

VÍ DỤ về tập tin **MEDIA.TXT[BASE]** đầy đủ:

```
GBWK27_07   20070621BASE      M01X03
M1,'UKHO Week 27_07 BASE MEDIA 1','Europe, Africa, and Middle East'
M1;B1,20070614,'Base Dataset 1',Europe',,
M1;B2,20070614,'Base Dataset 2','Africa',,
M1;B3,20070621,'Base Dataset 3','Middle East',,
```

4. Quản lý Media (Data Server)

Bản phát hành và phát hành lại của Base CD dựa vào quyết định của Data Server.Tuy nhiên, để ngăn chặnviệc đổi mới liên tục Base CD, các Bộ sản phẩm trao đổi riêng rẽ không được phát hành độc lập với nhau trên cùng CD.Tuy nhiên, có thể có trường hợp điều này là cần thiết, ví dụ sự ra đời của ENC từ một

17

quốc gia mới hoặc cần thiết quản lý Bộ sản phẩm trao đổi cập nhật.

Có khả năng Data Server sẽ vận hành một dịch vụ hai tầng, ví dụ họ sẽ hỗ trở cả hai dịch vụ CD-ROM và DVD.Thực hiện đầy đủ các khuyến nghị trong đoạn văn trên có thể không duy trì được tính đồng bộ giữa 2 cấp độ của dịch vụ do tính linh hoạt mà *large media*cung cấp. DVDs là trường hợp có thể lưu trữ nhiều dữ liệu và vì vậy nó không cần phát hành lại các media thường xuyên như là CD.

LƯU Ý:một Data Server phát hành Base CD bằng cách sử dụng tùy chọn *large media,* nhưng vì lý do chi phí, nên sẽ phát hành các bản cập nhật media trên CD. Trong những hợp này, cần đảm bảo nội dung và cấu trúc của bản cập nhật PHẢI phù hợp với Base media mà nó liên quan tới.

5. Quản lý Media

Các khối ENC tiếp tục gia tăng, việc cần một phương pháp tối ưu để tải chúng vào ECDIS/ECS là bắt buộc. Vì hầu hết khách hàng chỉ đặt mua ENC có sẵn, nên cần phải cẩn thận nhập các ENC đã mã hóa S-63 trực tiếp đề phòng các khách hàng nằm giữ giấy phép. Phần dưới đây minh họa các bước được đề nghị cho việc nhập dữ liệu ENC đã mã hóa:

- Chèn vào, đọc và xác nhận tập tin "**PERMIT.TXT**"
- Chèn vào "**Update CD**"
- Đọc danh sách sản phẩm "***FULL***" từ tập tin "**PRODUCTS.TXT**"
- Xác định và đánh dấu tất cả các cell đã đăng ký (đã có giấy phép hợp lệ)
- Xác định vị trí "**Base Media**" và "**BASE Exchange Set**" cho mỗi ENC được cấp phép
- Nhắc nhở người dùng cài đặt "**Base Media**" thích hợp.
- Cài đặt tất cả các ENC đã đăng ký từ "**Base Media**" và "**BASE Exchange Set**" liên quan
- Nhắc nhở người dùng chèn "Update Media" mới nhất để đưa ra tất cả các ENC cập nhật đã đăng ký và hoàn thành chu trình tải.

LƯU Ý: Trong trường hợp các dữ liệu ENC đã mã hóa không cần đọc tập tin CATALOG.031 hoàn chỉnh. Tập tin này chỉ nên được sử dụng để xác định vị trí mục tiêu của tất cả các ENC được cấp phép và các tập tin liên quan trong Bộ sản phẩm trao đổi.

6. Cảnh báo Media

Khi bản cập nhật media hàng tuần được tải lên Data Client phải kiểm tra xem ngày phát hành của tất cả các Base media là hiện có và cập nhật. "**STATUS.TXT**" trên Update CD mới nhất sẽ có ngày phát hành mới nhất của mỗi Base CD trong dịch vụ.

Nếu ECDIS/ECS không có Base CD mới nhất được tải lên thì một cảnh báo phải được thông báo cho người dùng tương tự như ví dụ sau:

"This 'Update Media' is not compatible with the actual installed 'Base Media'. Please install the following 'Base Media' first and then continue with the 'Update Media'."

<Field: User Information 1>

<Field: User Information 2>

<Field: User Information x> (where x is the base media

number)

“ ‘Update CD’ này không tương thích với ‘Base CD’ thực tế được cài đặt. Vui lòng cài đặt ‘Base CD’ đầu tiên và sau đó tiếp tục với ‘Update CD’ dưới đây.”

<Trường: Thông tin người dùng 1>

<Trường: Thông tin người dùng 2>

<Trường: Thông tin người dùng x> (ở đây, x là số Base CD).

Ví dụ:

“This ‘Update Media’ is not compatible with the actual installed ‘Base Media’. Please install the following ‘Base Media’ first and then continue with the ‘Update Media’.”

‘Base Media 2 dated 07 June 2007’ *tức là:*

“‘Update CD’ này không tương thích với ‘Base CD’ thực tế được cài đặt. Vui lòng cài đặt ‘Base CD’ đầu tiên và sau đó tiếp tục với ‘Update CD’ dưới đây.”

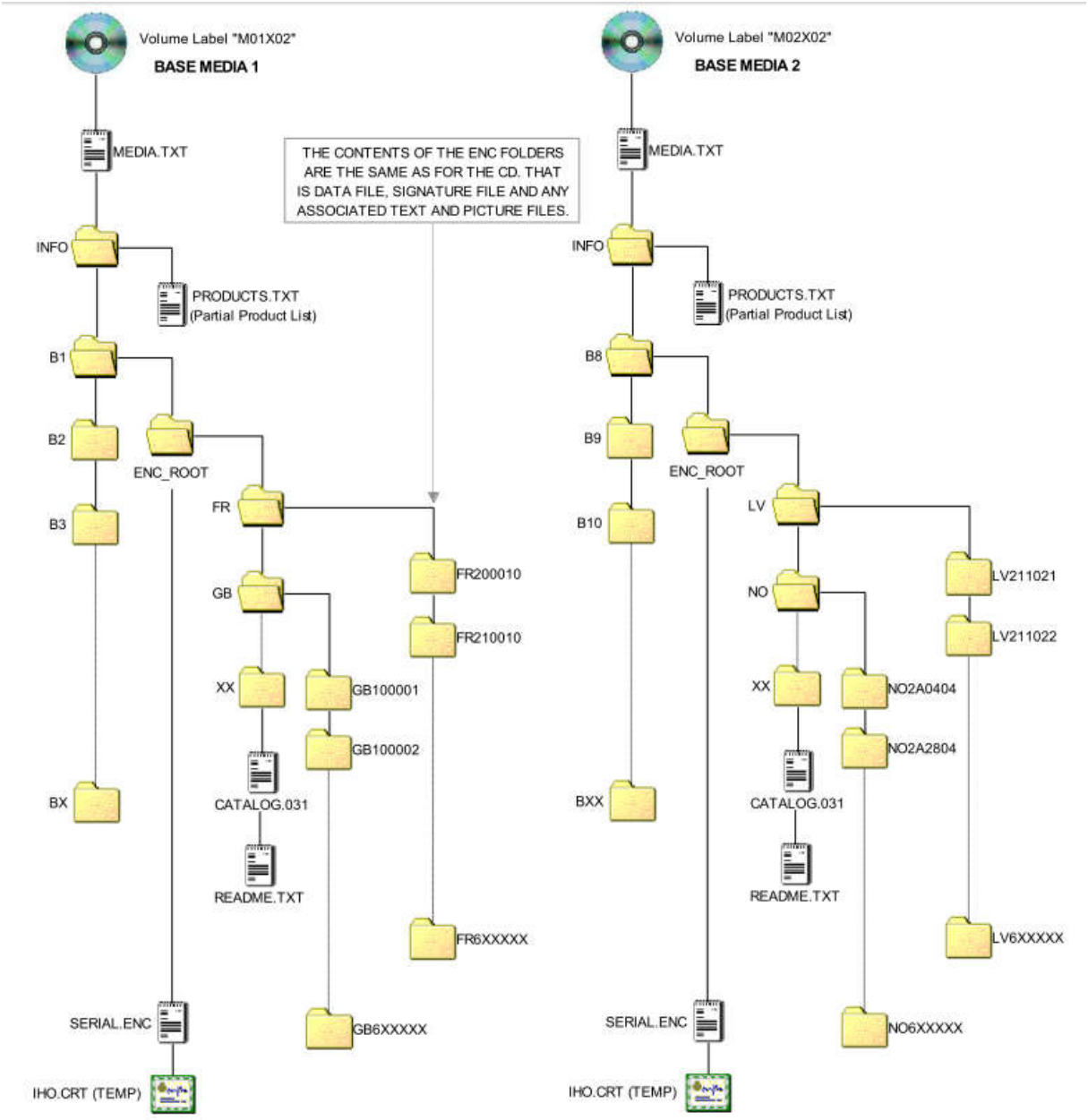
‘Base CD 2 ngày 07 tháng 6 năm 2007’

LƯU Ý: Người dùng sẽđược chỉ dẫn để cài đặt Base Media thích hợp có chứa các cell ENC được cấp phép.

PHỤ CHƯƠNG A

CẤU TRÚC TẬP TIN VÀ THƯ MỤC BASE MEDIA

Biểu đồ dưới đâyminh họa mức cao nhất cấu trúc tập tin và thư mục được sử dụng bởi Data Server khi cung cấp dịch vụ ENC đã mã hóa S-63 bằng cách sử dụng *DVD*. Tuy nhiên, cấu trúc dưới mỗi thư mục ENC_ROOT của Bộ sản phẩm trao đổi có thể thay đổi giữa các Data Server.

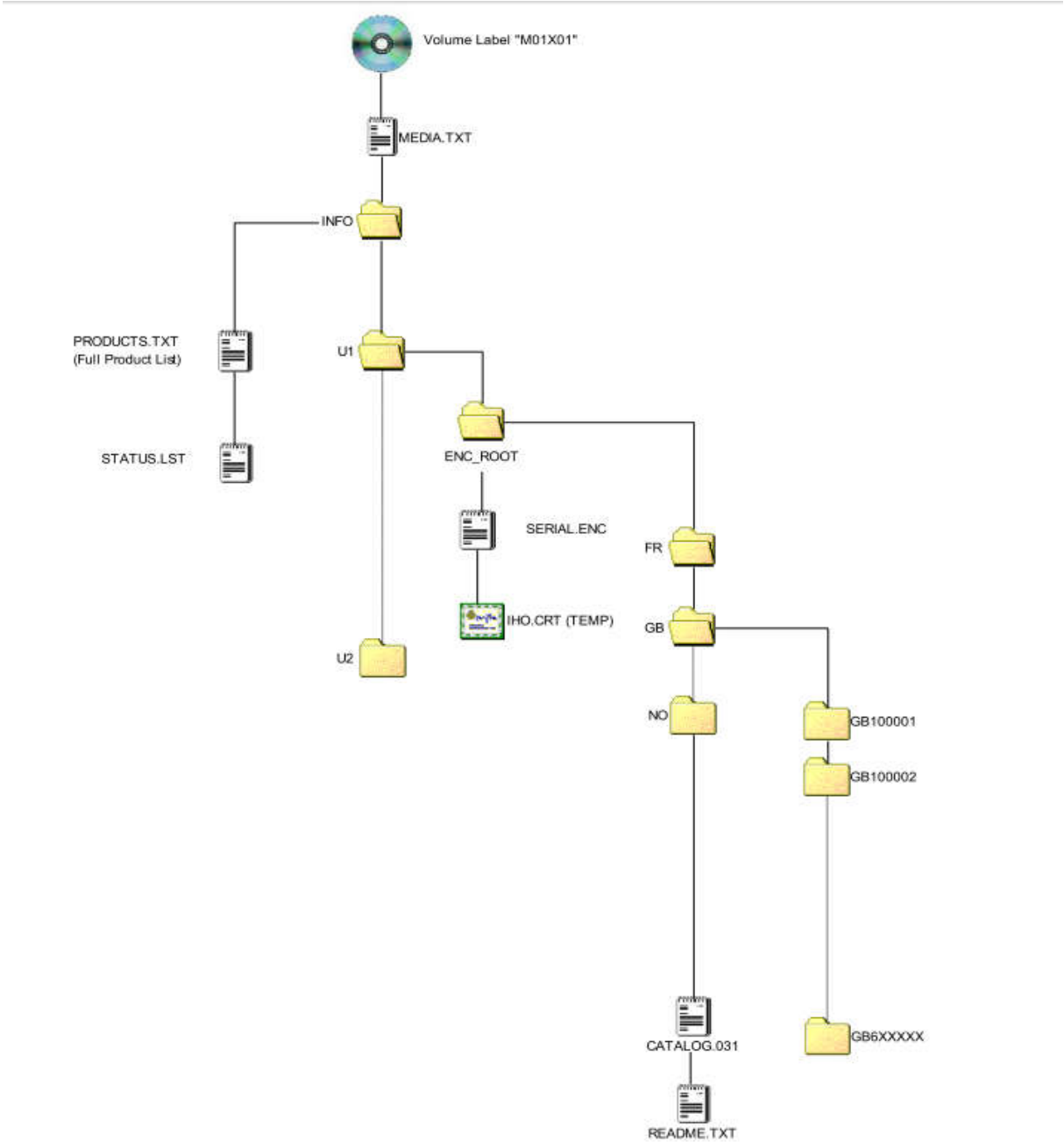


LARGE MEDIA SUPPORT FOR S-63 ENCRYPTED ENC SERVICES
BASE MEDIA FOLDER AND FILE STRUCTURE

PHỤ CHƯƠNG B

CẤU TRÚC TẬP TIN VÀ THƯ MỤC UPDATE MEDIA

Biểu đồ dưới đâyminh họa mức cao nhất cấu trúc tập tin và thư mục được sử dụng bởi Data Server khi cung cấp dịch vụ ENC đã mã hóa S-63 bằng cách sử dụng *DVD*. Tuy nhiên, cấu trúc dưới mỗi thư mục ENC_ROOT của Bộ sản phẩm trao đổi có thể thay đổi giữa các Data Server.



UPDATE MEDIA STRUCTURE
(Only top level folders & files)