

S-63 암호화된 전자해도 공급을 위한 지원시스템 개발연구

† 오세웅* · 장원석* · 박종민* · 박한산* · 서상현*

*한국해양연구원 해양시스템안전연구소

A Study on the Development of Supporting System for Distribution of S-63 ENCs

† Sewooong Oh* · Wonseok Jang* · Jongmin Park* · Hansan Park* · Sanghyun Suh*

*Korea Ocean Research & Development Institute, Maritime & Ocean Engineering Research Institute, Daejeon 305-343, Korea

요약 : 정보통신 시대에 정보 보안은 중요하며 특히 전자해도 등 수로데이터 분야에 있어서 매우 중요한 문제이다. 경제적 효과를 배제하고 해도정보의 불법적인 사용은 항해안전에 치명적인 오류를 발생시킬 수 있으므로, 전자해도 국제공급센터 및 해도공급기관은 정보보호를 위한 방안을 연구하였다. 국제수로기구인 IHO에서는 전자해도 보안에 대한 단일의 방안을 마련하여 S-63 표준으로 수립한 바 있다. 우리나라 전자해도 생산 및 공급을 담당하는 국립해양조사원은 이러한 전자해도 보안 적용이 요구되는 바, IHB 중심의 보안체계가입을 위해서는 보안체계를 분석하고 이를 지원할 수 있는 보안시스템의 개발이 필요하다. 본 연구에서는 S-63 기반 보안체계를 분석하고 데이터 서버로서 역할을 하기 위한 지원시스템을 개발하였다.

핵심용어 : 전자해도, 보안체계, 수로데이터전송표준, 수로데이터보안표준, 전자해도표시시스템, 국제수로기구

ABSTRACT : Copyright infringement and data piracy are pervasive problems of digital era and Electronic Navigational Charts(ENC) are not free from these issues. Aside from the economic impact, the unofficial distribution of nautical information has significant safety concerns. Therefore, official distributors of nautical information have sought appropriate methods to protect their data and to provide the mariner with a certificate of authenticity through the adoption of security schema. However, a plethora of different security schema provided by independent distributors markedly complicates the software development of Electronic Chart Display and Information Systems (ECDIS) manufacturers and makes it more difficult to achieve the goal of seamless world-wide electronic navigational database easily accessible to the mariner. A fundamental concern of IHO is that adoption of a single, centrally administered security scheme for all ENCs could improve the ease of use of ENCs and enhance safety of navigation. IHO have driven protection scheme as S-63, S-63x. NORI(National Oceanographic Research Institute) necessarily need protection scheme and supporting system for nautical information. This paper presents protection scheme for NORI and proposes support system for ENC protection.

KEY WORDS : ENC, Sevcurity Scheme, S-57, S-63, ECDIS, IHO

1. 서 론

우리나라 전자해도는 1995년 시험제작과 2001년 공급을 시작으로 전자해도표시시스템(ECDIS) 뿐만 아니라 각종 간이전자해도시스템(ECS)에 사용되어 선박의 안전항해에 필수 인프라로 인식되고 있으며, 최근 논의되고 있는 E-Navigation 전략의 핵심 항목으로 선정됨에 따라 전자해도의 정확성과 최신성이 강조되고 있다. 그러나 현재의 전자해도 공급체계는 전자해도 공급 이력관리가 취약하고, 전자해도가 탑재되는 ECDIS의 종류 및 특징 분석이 부족하며 전자해도의 불법 복제 및 변환에 대한 우려가 지적되고 있다. 본 연구에서는 이를 해결하기 위해 국제수로기구, 데이터 서버, ECDIS 생산자, 전자해도 사용자로

구성된 전자해도 공급 및 보안체계를 제시하며, 전자해도 데이터 서버의 입장에서 사용자 이력관리 및 보안체계 지원을 위한 시스템을 개발하였다.

2. 전자해도 공급 현황

우리나라의 전자해도는 종이해도와 동일하게 총 212종으로 국립해양조사원에서 생산 및 유지관리를 하며 항행통보에 대한 업데이트 정보를 제공하고 있으며, 두 곳의 전자해도 판매대행업체를 두어 판매대행을 담당하도록 하고 있다. 전자해도의 주요 고객인 ECDIS 사용자는 전자해도 판매대행업체에 구매요청하면, 판매대행업체는 전자해도명, 라이센스 기간, ECDIS 장비

정보가 포함된 매수 신청서를 작성하여 국립해양조사원에 제출 한다. 국립해양조사원에서는 해당 전자해도를 카탈로그 파일이 포함된 교환셋(Exchange set)을 구성하여 판매대행업체에 전달 하면 판매대행업체는 CD 매체로 포장하여 ECDIS 사용자에게 공급하게 된다.

3. 전자해도 보안체계

3.1 국제수로기구 보안체계

국제수로기구에서는 전자해도와 같은 디지털 컨텐츠 불법 복제 및 변환을 방지하기 위해 IHO 기술위원회 산하 DPSWG (Data Protection Scheme Working Group)을 조직하였다. DPSWG는 북유럽 전자해도공급센터인 Primar Stavanger가 개발한 전자해도 보안체계를 적극 수용하여 S-63의 이름으로 전자해도 보안체계를 수립하였다. S-63은 보안체계의 구성원과 각 구성원의 역할 및 절차, 암호화 복호화 방법에 대해 기술하였다. S-63 보안체계 각 구성원의 관계는 Fig. 1과 같다.

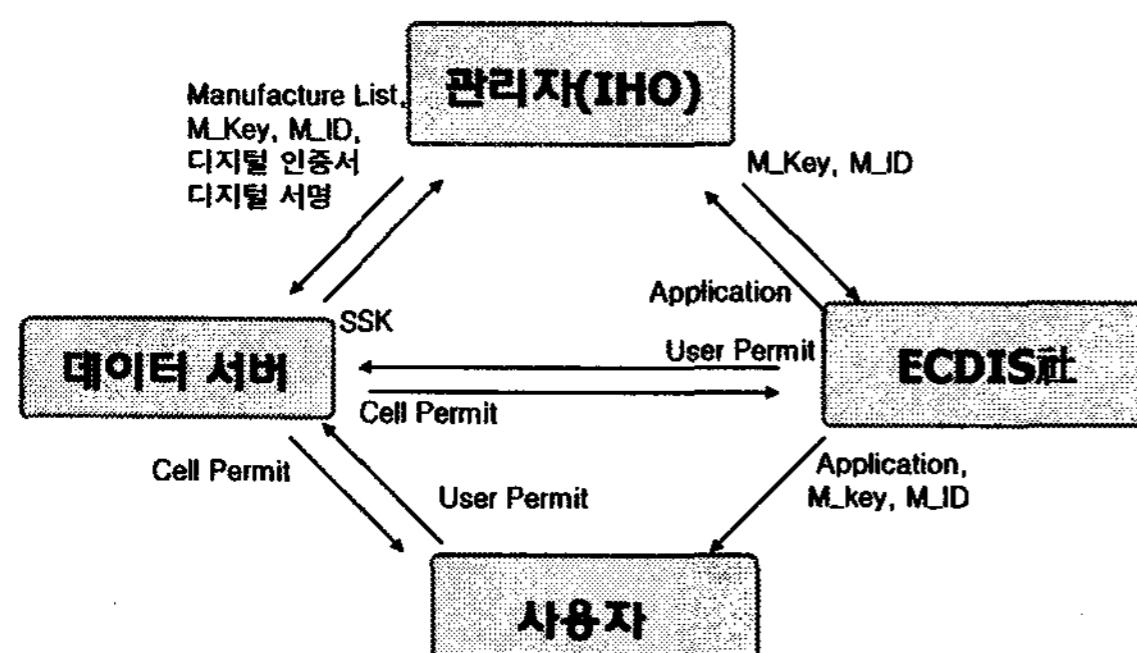


Fig. 1 IHO S-63 Protection Scheme

3.2 국내 전자해도 보안체계 수립 방안

국내 보안체계 수립을 위해 데이터 서버, ECDIS社, 사용자 측면에서 방안을 제시하였다.

(1) 데이터 서버 측면

국내에서 전자해도의 제작과 유지관리를 담당하고 있는 국립해양조사원이 데이터 서버 역할을 맡으며, 관리자인 IHO에 데이터 서버로서 지원을 받기 위해서는 데이터 서버 계약 및 보안지원시스템이 구축되어야 한다. 보안 지원시스템의 역할은 크게 세 가지로 첫째 SSK 생성, 관리자/데이터 서버 인증서, ECDIS社 목록 처리 등의 보안지원시스템 초기 설정기능이 필요하며, 둘째 암호화된 Base CD 생성, 전자해도 사용 승인을 위한 Cell permit 생성 등의 전자해도 관리기능, 셋째로 공급한 전자해도의 명세 및 사용자 관리를 위한 이력관리 기능이 필요하다. 현재 IHO에 등록된 RENC 및 수로국은 SevenCS, UKHO 등을 포함하여 14개 기관으로, 국립해양조사원은 보안 지원시스템을 개발하여 IHO에 데이터 서버로서의 등록이 요구된다.

(2) ECDIS社 측면

현재 IHO에 등록된 ECDIS社는 88개 사로 우리나라의 경우 이마린로직스, 삼성중공업을 포함하여 5개사가 등록되어 있다. 전자해도 보안체계가 활성화 될 경우 IHO에 등록된 ECDIS 만이 전자해도를 수용할 수 있으므로 ECDIS 및 ECS를 제작하고 있는 국내기업은 IHO로의 ECDIS社 등록이 요구된다.

(3) 사용자 측면

현재의 전자해도는 ECDIS에서 뿐만 아니라 해양GIS 목적으로 사용되고 있으나 전자해도 보안체계가 도입될 경우 전자해도의 ECDIS 이외의 사용은 금지될 것으로 예상된다. 전자해도의 GIS 목적으로의 사용은 IHO에서 개발 중인 S-100 표준을 통해 가능하며, ECDIS 사용자는 보안체계를 통해 정확하고 안전한 업데이트를 보장받게 될 것으로 사료된다.

4. 전자해도 보안 지원시스템 개발

본 프로그램을 개발하기 위해 개발도구로 JavaSE v1.4와 Eclipse를 사용하였고 MS Windows XP 운영체제에서 테스트하였다. 본 프로그램에서는 작업자 환경의 친숙도를 높이기 위해 현재 전자해도 교환셋 생성에 사용되고 있는 ENC Manager와 유사한 User Interface를 채택하였다. 메인 화면은 다음과 같다.

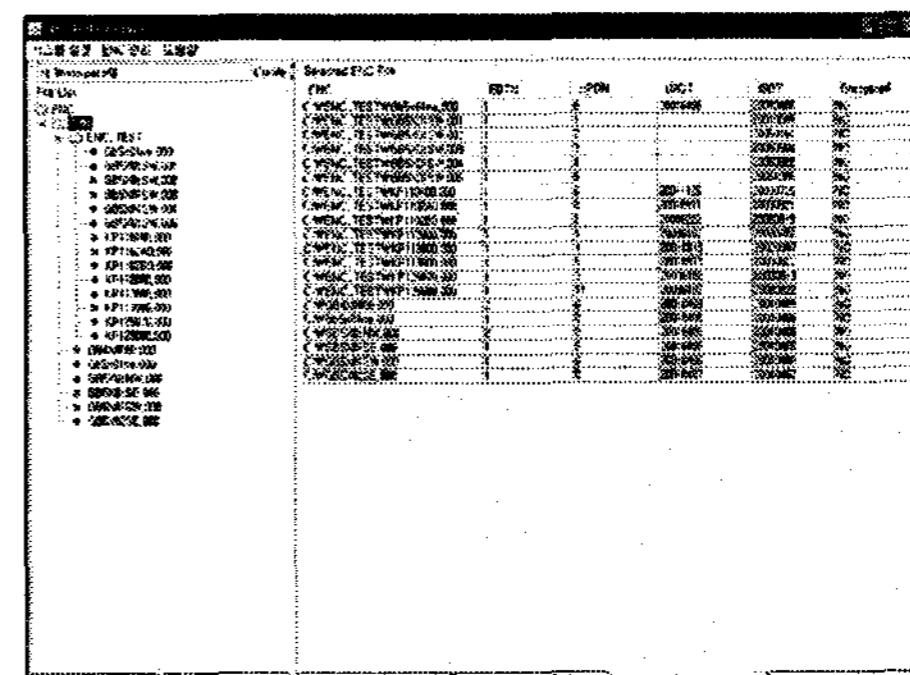


Fig. 2 Main User Interface of Supporting System

(1) 시스템 초기 설정부분

데이터 서버가 절차상 보안 지원시스템 사용을 위한 초기설정 부분으로 데이터 서버의 공개키에 서명한 SSK를 생성하고 관리자인 IHO로부터 받은 데이터서버 인증서, 관리자 인증서를 저장하며, ECDIS社 목록을 저장하는 기능이 포함된다. 다음은 각 기능의 개발화면이다.

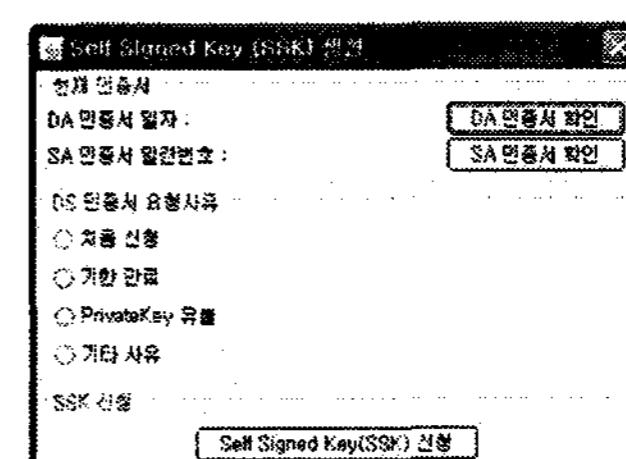


Fig. 3 Generation of Self Signed Key(SSK)

Fig. 4 List of Self Signed Key(SSK)

Fig. 8 List of Cell Permit

ES-Demo Server) 防護規則名稱	子層級子規則名稱	SAC 處理
2004-10-05	IP端口	封鎖端口
2004-10-05	IP地址	封鎖IP
2004-10-05	IP子網	封鎖子網
2004-10-05	MAC地址	封鎖MAC
2004-10-05	MAC子網	封鎖MAC子網
2004-10-05	MAC子端口	封鎖MAC子端口
2004-10-05	MAC子子端口	封鎖MAC子子端口
2004-10-05	MAC子子子端口	封鎖MAC子子子端口
2004-10-05	MAC子子子子端口	封鎖MAC子子子子端口

Fig. 5 List of certification for data server

No.	M.LK..	Cont..	Re..	Organiz..	Contact	Country	Tel	E-mail
21	11294	OK		internation..	Michel H..	MONACO	+377 93108..	pac@ihb.mc /..
22	11295	OK		internation..	Michel H..	MONACO	+377 93108..	pac@ihb.mc /..
23	11296	OK		internation..	Michel H..	MONACO	+377 93108..	pac@ihb.mc /..
3130	313031..	status	2004..	e-MLK	Young Kim	Korea	042-365-1067	reese@embx.c..

Fig. 6 List of ECDIS OEM

(2) 전자해도 관리 부분

암호화된 전자해도 Base CD를 생성하고 사용자의 구매 요청에 대한 Cell permit을 생성하는 부분으로 구성된다. Fig. 11의 메인 화면을 중심으로 좌측의 전자해도 DB에서 전체 파일을 선택하면 Base CD가 생성되며, 사용자가 구매 요구한 전자해도를 일부 선택하여 Cell permit을 생성하게 된다. 본 프로그램에서는 기 사용되고 있는 ECDIS 중 S-63 보안체계를 지원하지 않는 장비가 있을 것으로 사료되어 비암호화 교환셋 생성 기능을 추가하였다.

B-57 EMC 관리 선택			
선택 항목	C:W1	선택 항목	C:W1
B-57 EMC			
회원명	Edison	Update	결제
KP10000.000	1	6	EMC
KP1100A1000	1	6	EMC
KP10000.000	1	2	EMC

Fig. 7 Generation of Cell Permit

정보 분야에서는 저작권 침해 및 불법 사용을 방지하기 위한 다양한 방안이 개발되었고, 전자해도를 포함한 수로정보 분야 역시 국제수로기구 주도로 보안체계를 준비하여 추진 중에 있다. 현재 우리나라 전자해도 공급체계는 전자해도 공급 이력관리가 취약하고, 전자해도가 탑재되는 ECDIS의 종류 및 특징 분석이 부족하며 전자해도의 불법 복제 및 변환에 대한 우려가 지적되고 있다. 이를 개선하기 위해 본 연구에서는 전자해도 공급체계 개선 및 보안지원을 위한 방안을 분석하고 국립해양조사원이 전자해도 데이터 서버로서 등록을 위해 필요한 보안지원 시스템을 개발하였다. 본 논문의 연구 결과는 전자해도 데이터의 공신력 확보, 데이터 생산자 및 공급자의 안정적인 서비스 체계 구축, 전자해도의 활용 증진 등에 기여할 것으로 사료된다.

후기

본 논문은 국립해양조사원의 연구과제인 “차세대 전자해도 기술개발” 과제로 수행 되었습니다.

참고문헌

- [1] IHO S-57, IHO Transfer Standard for Digital Hydrographic Data.
 - [2] IHO S-62, IHO Codes for agencies Producing S-57 Data.
 - [3] IHO S-63, IHO Data Protection Scheme.
 - [4] IHO S-63, S-63 Test Data Implementation Guide v1.1.