2014년도 공동학술대회 논문집 pp. 284~286

전자해도 시스템 관점에서의 전자해도 보안 표준(S-63) 적용 방안 연구

† 조경민 · 오세웅* · 심우성*

†,*한국해양과학기술원 부설 선박해양플랜트연구소

요 약 : 국제수로기구(IHO: International Hydrographic Organization)는 전자 해도의 불법 복사와 사용을 방지하기 위해 전자해도 보안 표준(IHO Data Protection Scheme, Edition 1.1.1 - April 2012, IHO Publication S-63)을 제정한 바 있으며, 국제적으로는 보안체계가 적용된 암호화된 전자 해도가 공급되고 있다. 국립해양조사원에서 국내 사용을 위해 공급하는 전자 해도에는 보안 표준을 적용하지 않다가 2014년부터 전자 해도의 비 항해 목적으로의 사용을 방지하기 위해 보안 표준 적용과 함께 비 항해용 해도 정보를 제공하고 있다. 따라서 전자해도 시스템 관점에서 전자 해도를 사용하기 위해서는 전자해도 보안 표준에 대한 높은 지식이 요구되고 있다. 이에 본 연구에서는 전자해도 보안 표준과 체계를 분석하고, 표준에서 제공하는 전자해도 보안 표준 테스트 데이터를 전자해도 시스템 관점에서 시험하였다. 이를 통해 보안 모듈과 전자해도 시스템과의 관계를 소프트웨어 구조 관점에서 제시하고 표준을 적용할 때 필요로 하는 표준 접근 절차와 방법을 연구결과로 제시 하였다.

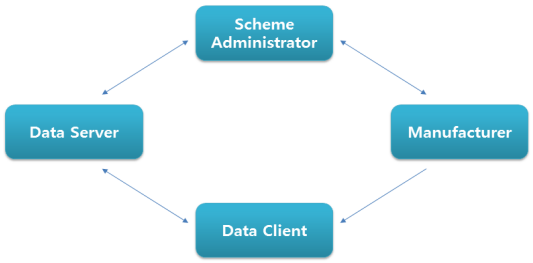
핵심용어 : 전자해도, S-63, ECS, ECDIS

1. 서론

- 국제수로기구(IHO: International Hydrographic Organization)는 전자 해도의 불법 복사와 사용을 방지하기 위해 전자해도 보안 표준(IHO Data Protection Scheme, S-63)을 제정
- 국제적으로 보안체계에 따라 암호화된 전자 해도가 공급되고 있음
- 국립해양조사원에서 국내에 공급한 전자 해도에는 보안 표준을 적용하지 않다가 2014년부터 보안 표준을 적용하고 있음
- 전자해도 활용 시스템에서 국립해양조사원이 보안체계를 적용하여 공급한 전자 해도를 사용하기 위해서는 보안 표준한 지식이 요구됨
- IHO S-63 보안 표준에 대해 분석하고 전자해도 시스템 적용에 필요한 절차 등의 고려사항을 논함

2. S-63 정의 및 구조

- S-63의 정식 명칭은 "S-63 IHO Data Protection Scheme" 이며 전자해도를 보호하기 위한 보안 구조와 운영 절차 등을 포함하는 권고 표준



3. Scheme Administrator(SA)

- S-63에서 Scheme Administrator(SA)는 오직 하나만 존재 가능
  - SA는 S-63의 유지 보수와 보안 정책의 참여자를 통합 및 조정하는 역할
- 국제수로사무국(IHB: The International Hydrographic Bureau)이 현재 SA의 역할을 수행
  - S-63에 관련된 모든 문서를 관리
  - 최상위 디지털 인증서를 관리
- 유일하게 S-63의 다른 참여자의 신원을 확인할 수 있음

4. Data Server

- 전자 해도를 암호화하고 서명하는 역할
- 허가된 Data Client에게 전자해도 라이선스를 발급
  - Data Client는 라이선스를 통해서 전자 해도를 복호화
- 발행한 라이선스가 특정 EPS(Electronic Process System)에서만 사용되기 위해서 각 EPS의 HW_ID를 이용하여 전자 해도 암호화
- 각국의 수로국, Value Added Resellers, RENC 등이 데이터 서버의 역할을 함

† 조경민 : gmjo@kriso.re.kr 010-2032-0311

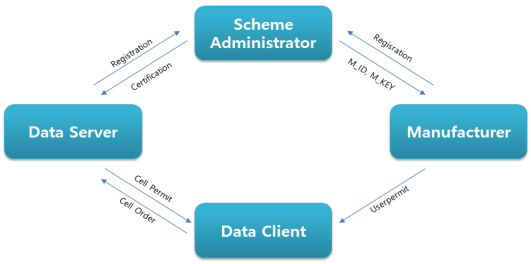
5. Original Equipment Manufacturers(OEM)

- IHB S-63 Data Protection Scheme에 등록된 EPS 제조사
- SA로부터 고유한 M_ID, M_KEY를 받음
  - M_ID는 공개
  - M_KEY는 비공개

6. Data Client

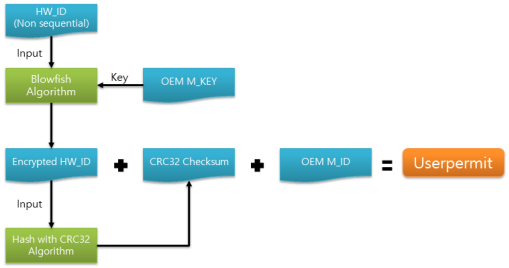
- 전자 해도의 최종 사용자
  - ECDIS/ECS를 사용하는 항해사
- Data Server로부터 암호화된 전자 해도를 받아 사용
- Data Client의 EPS(Electronic Process System)가 전자 해도 전자 서명을 증명하고 전자 해도의 복호화 수행

7. S-63 Protection Scheme Relationship



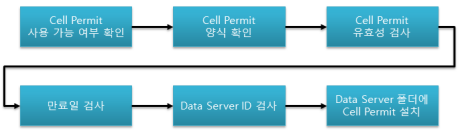
8. OEM & Data Client Processes
- EPS제작 시 Userpermit 생성 과정

- Userpermit은 OEM이 판매하는 EPS마다 부여하는 고유 식별자



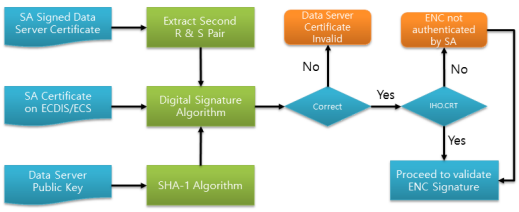
8. OEM & Data Client Processes
- ENC Cell Permit 설치

- Cell Permit은 전자 해도를 구매할 때 Data Server로부터 발행
- 구매한 전자 해도를 복호화 하는데 사용



8. OEM & Data Client Processes
- 전자해도 인증 및 완전성 검사

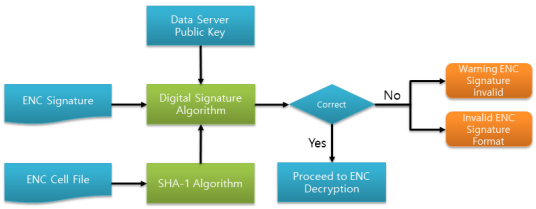
- Data Client 시스템은 암호화된 전자 해도 인증 및 완전성 검사를 해야 함



SA가 Data Server 인증서를 증명하는 과정

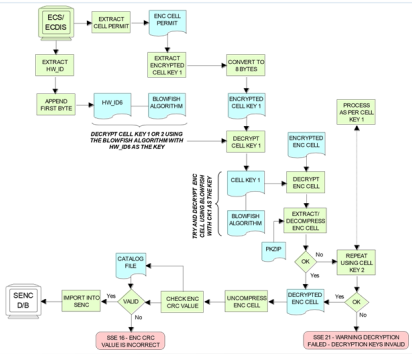
8. OEM & Data Client Processes
- 전자해도 인증 및 완전성 검사

- Data Client 시스템은 암호화된 전자 해도 인증 및 완전성 검사를 해야 함



전자해도 파일에 대한 전자 서명을 확인하는 과정

8. OEM & Data Client Processes
- 전자해도 및 업데이트 파일 복호화



8. OEM & Data Client Processes
- Data Client에 대한 지속적인 경고

- S-63에서는 기한이 지난 데이터가 사용될 수 있음
- 이때 Data Client는 Viewer화면에 지속적인 경고를 표출하여야 함

- 전자해도 권한의 기한이 만료된 경우

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

- 기간이 지난 SENC 인 경우

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

8. OEM & Data Client Processes
- Quality Assurance for Data Client

- Data Client QA 절차

SA 전자 인증서 승인 및 검사

↓

Userpermit 생성

↓

Data Server 전자 인증서 검증

↓

Cell Permit 확인

↓

전자 해도 인증 및 복호화

8. OEM & Data Client Processes
- Quality Assurance for Manufacturers

- Manufacturers QA 절차

기밀유지서약서에 동의

↓

테스트 데이터를 통한 시스템 테스트

↓

M_ID 및 M_KEY 보관

↓

HW_ID 생성

↓

HW_ID 기록

9. 결론

- 전자해도 시스템에 S-63을 적용하기 위한 절차 및 방법 분석

- 필요한 알고리즘
  - Blowfish
  - CRC32
  - SHA-1
  - DSA(Digital Signature Algorithm)

- S-63을 위한 소프트웨어는 전자 해도 시스템과 별도로 Userpermit 및 HW_ID를 통해 운영 됨