S-63 IHO Data Protection Scheme Explained

Friedhelm Moggert-Kägeler,
SevenCs GmbH

HYDRO 2010,
2 - 5 November 2010,
Rostock, Germany

S-63 IHO Data Protection Scheme

Background
IHO S-63 - Background

• Protection of ENC information.
• Edition 1.1 was released in March 2008.
• Based on Primar protection scheme.
• Adopted as IHO standard in 2001.

• Piracy Protection:
  – To prevent unauthorised use of data.

• Selective Access:
  – To restrict access according to a licensing scheme.

• Authentication:
  – Assurance that data is from approved sources.
S-63 – Participant Relationships

Scheme Administrator
IHO: Coordination, Maintenance and Control

Data Server: Supplier of ENCs

Data Client: End User of ENCs

OEM: ECDIS Manufacturer

Data Server ↔ Data Client

• **End User** gets ENCs from ENC supplier.
• Supplier must be trustworthy.
• Means to verify ENC suppliers identity.
• Proof of suppliers trustworthiness
  – Certification by „higher authority.“
Data Server: Supplier of ENCs

Data Client: End User of ENCs

STOP! Chart has not been signed.

Data Server

Data Client

THE SOURCE OF ECDIS

S-63 Explained, HYDRO 2010, 2 - 5 Nov. 2010, Rostock

7

Data Server

Data Client

THE SOURCE OF ECDIS

S-63 Explained, HYDRO 2010, 2 - 5 Nov. 2010, Rostock

8
Data Server: Supplier of ENCs

Data Client: End User of ENCs

STOP! Signature has not been verified.
Data Server ➔ Data Client

Data Server: Supplier of ENC

Data Client: End User of ENC

Must have a Bona Fide Certificate

Data Server ➔ IHO

- ENC supplier contacts IHO.
- Asks for confirmation of bona fide status.
- Agrees to accept conditions and procedures to proof trustworthiness.
- Receives bona fide certificate.
Data Server  ➞  Data Client

Data Server:
Supplier of ENCs

Data Client:
End User of ENCs

Certificate was signed by the Certifying Authority (IHO)

Signature of ENC Supplier is shown on Certificate

Must have a Bona Fide Certificate

STOP!
Is the Certificate genuine?

S-63 Explained, HYDRO 2010-2 - 5 Nov. 2010, Rostock
Data Server ➔ Data Client

Data Server: Supplier of ENCs

IHO (Certifying Authority)
Publicates Signature

Data Client: End User of ENCs

Must have a Bona Fide Certificate

S-63: IHO.CRT

S-63 Explained, HYDRO 2010, 2 - 5 Nov. 2010, Rostock
Data Server ➔ Data Client

Data Server:
Supplier of ENC data.

- Must have a Bona Fide Certificate

Data Client:
End User of ENC data.

- Authentication was successful!

ENC Supplier provides ENC data.

- Has an interest to protect ENC data:
  - Prevent unauthorised use.
  - Selective access (for licensed end users.)

- ENC Supplier encrypts ENC information.

- Provides decryption keys.
Data Server ➔ Data Client

Data Server: Supplier of ENCs

Data Client: End User of ENCs

Data Server ➔ Data Client

Data Server: Supplier of ENCs

Data Client: End User of ENCs

S-63: Cell Key

S-63: Encrypted ENC
Data Server ➔ Data Client

Data Server: Supplier of ENCs

Data Client: End User of ENCs

IHO (Certifying Authority)

Provides additional box

S-63: Hardware Id

S-63: Manufacturer Key

S-63: Manufacturer Key

S-63 Explained, HYDRD 2010-2 - 5 Nov. 2010, Rostock

THE SOURCE OF ECDIS
Data Server ➔ Data Client

Data Server: Supplier of ENCs
Data Client: End User of ENCs

S-63 Explained, HYDRO 2010, 2 - 5 Nov, 2010, Rostock

Data Server ➔ Data Client

Data Server: Supplier of ENCs
Data Client: End User of ENCs

S-63: Manufacturer Key
S-63: User Permit

S-63 Explained, HYDRO 2010, 2 - 5 Nov, 2010, Rostock
Data Server ➔ Data Client

Data Server: Supplier of ENC

Data Client: End User of ENC

Data Server ➔ Data Client

Data Server: Supplier of ENC

Data Client: End User of ENC
Data Server ➔ Data Client

**Data Server:** Supplier of ENC

**Data Client:** End User of ENC

S-63 Explained, HYDRO 2010, 2 - 5 Nov. 2010, Rostock

S-63: Decrypted Hardware Id

S-63: Cell Key
Data Server ➔ Data Client

Data Server: Supplier of ENC(s)

Data Client: End User of ENC(s)

S-63: Cell Permit

S-63 Explained, HYDRO 2010.2 - 5 Nov. 2010, Rostock
Data Server ➔ Data Client

Data Server: Supplier of ENC

Data Client: End User of ENC

S-63: De-encrypted Cell Permit

S-63 Explained, HYDRO 2010, 2 - 5 Nov. 2010, Rostock
Data Server ➔ Data Client

Data Server: Supplier of ENC

Data Client: End User of ENC

S-63: De-crypted Cell

Chart was successfully decrypted

S-63 Explained, HYDRO 2010, 2 - 5 Nov 2010, Rostock

www.sevenecs.com
S-63 Protection - Summary

- ENCs are digitally signed to authenticate the data supplier (end user’s interest.)
- ENCs are encrypted for copy protection reasons (ENC supplier’s interest.)
- Signature creation and data encryption are independent.
- Different encryption methods.
- Both are based upon a hierarchical “encryption chain” with the IHO at the top.
Thank you very much for your attention!

Contact: Friedhelm Moggert-Kägeler
SevenCs GmbH, Hamburg
mo@sevenscs.com