ic-enc.org
International Centre for ENCs

Peter Jones, UKHO

S-63 Background

- S-63 is the IHO Data Protection Standard
- Evolved from the previous “Primar Security Scheme” designed to protect the Primar Official ENC Service
- S-63 is made up of two basic elements:
  - Data Encryption
  - Data Authentication

S-63 Background

- Encryption allows the supplier to control who can access which ENC products (selective availability) and for how long. So protects against unlicensed use.

- Authentication allows the customer to confirm the source of the data is legitimate, and to confirm the data has not been corrupted (complements existing CRC check)

- S-63 therefore also protects the mariner from data corruption (either malicious or accidental) which would affect their safety and compliance to SOLAS carriage requirements

S-63 Background

- Problems now exist moving:
  - From a scheme designed to protect one service;
  - To an international standard designed to protect many services

- OEMs have all implemented the former PSS subtly differently, with some systems only designed to handle data from a single service at a time – so are not now well suited to S-63

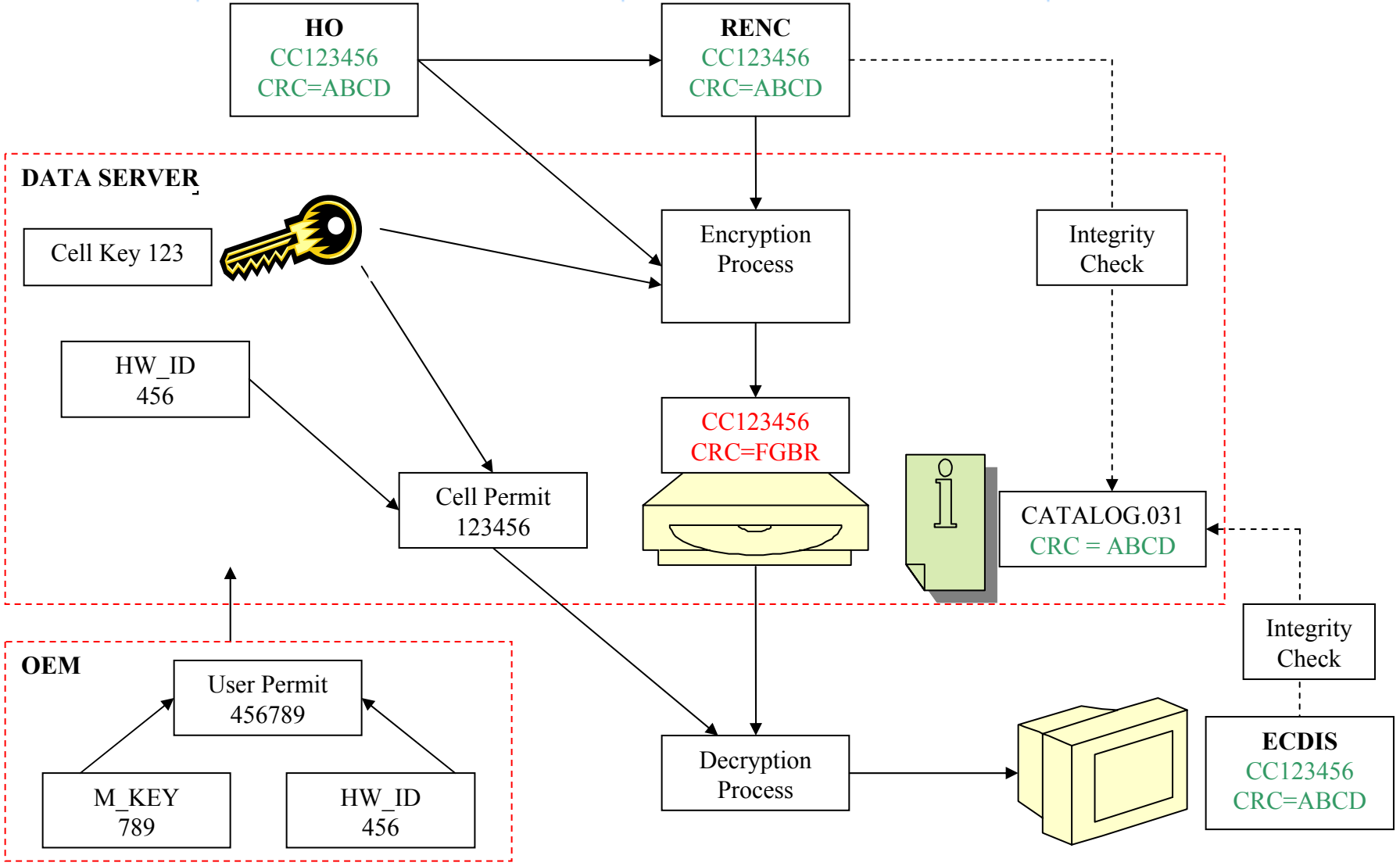
- S-63 working group has developed guidelines for OEMs and Data Servers on how they should implement S-63 to ensure data services protected using S-63 will work correctly on ECDIS systems

S-63 Basics - Encryption

- Encryption scrambles the ENC cell in a specific way, using the Blowfish algorithm
- The resultant file is unreadable unless you have the relevant permit to unscramble the file
- The permit decrypts the scrambled file, restoring it back to its original form

S-63 Basics - Encryption

- Each cell is encrypted using a different “Cell Key”
- Each target display system (e.g. ECDIS) contains a different “Hardware ID”
- A permit contains details of a particular Cell Key and Hardware ID, plus a subscription end-date, and so only decrypts a file if:
  - The cell key matches (i.e. correct ENC cell)
  - If the Hardware ID matches (i.e. correct ECDIS system)
  - The system date pre-dates permit expiry date (i.e. current subscription period
- The permit therefore controls the licence the customer purchases and is an integral part of any integrated end-user service.

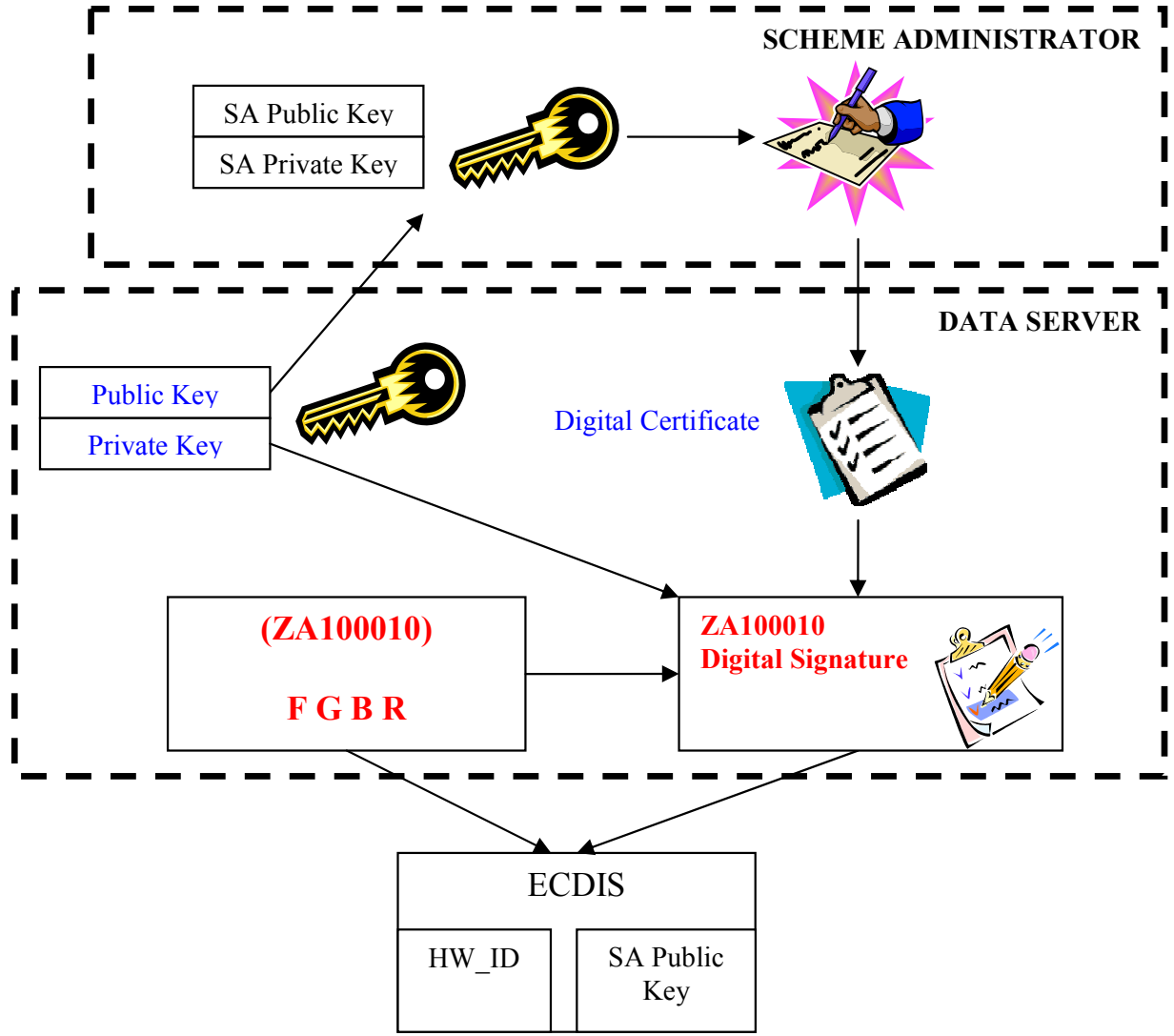

HO
CC123456
CRC=ABCD
RENC
CC123456
CRC=ABCD
DATA SERVER
Cell Key 123
Encryption Process
Integrity Check
HW_ID
456
CC123456
CRC=FGBR
Cell Permit
123456
CATALOG.031
CRC = ABCD
Integrity Check
OEM
User Permit
456789
M_KEY
789
HW_ID
456
Decryption Process
ECDIS
CC123456
CRC=ABCD

S-63 Basics - Authentication

- Authentication allows a customer to confirm that the ENC has originated from a bone fide source, and to know this source (i.e. the Data Server)
- This is achieved by providing a digital signature file together with the encrypted ENC cell it authenticates
- Only registered Data Servers can produce valid digital signatures since they first need to receive a digital certificate from the scheme administrator (IHB).

S-63 Basics - Authentication

- If the encrypted ENC file has been changed in any way (by accident or otherwise), the digital signature will no longer authenticate the ENC.
- Authentication therefore also lets the customer know if the file is corrupted.
- This is in addition to the existing CRC check ECDIS systems already perform after the cell is decrypted, and which identifies accidental data corruption.


SCHEME ADMINISTRATOR
SA Public Key
SA Private Key
DATA SERVER
Public Key
Private Key
Digital Certificate
(ZA100010)
F G B R
ZA100010
Digital Signature
ECDIS
HW_ID
SA Public Key

Trusted Parties

- Data Servers manage the encryption, signing and permit generation processes.
- They therefore need to know the manufacturer keys used by OEMs so that they can successfully generate permits for their customers
- This information enables them to calculate the “Cell Keys” used to encrypt an ENC; so they are also able to decrypt already encrypted ENCs.
- OEMs also know their own manufacturer key so that they can produce user permits for customers who purchase their S-63 compatible display equipment
- OEMs can therefore calculate the “Cell Keys” used to encrypt an ENC; so they are also able to decrypt already encrypted ENCs

Trusted Parties

- Both Data Servers and OEMs are therefore in responsible positions of trust since they:
  - Manage the encryption and permit generation process
  - Control how decrypted data is stored within target system
  - Are able to decrypt already encrypted data if they choose
  - Are assigned the role of authenticating that ENC data originates from a legitimate source

- The confidential information Data Servers and OEMs receive from the scheme administrator (IHB) are controlled through confidentiality agreements

- Data Servers must be sponsored by a relevant government organisation (e.g. HO, RENC) before they can sign such an agreement.

Trusted Parties

- The work performed by Data Servers and OEMS is vital to the successful development of integrated services
- Data Servers must purchase from a number of different suppliers to develop an integrated service
- They therefore need to be supported by the HO community and given the maximum flexibility and independence of operation to perform their role successfully.
- This is even more true today due to the S-63 implementation issues which still exist.