

### **PRIMAR support to IHO**

#### **Protection Scheme Administrator (SA)**

Operated by the Norwegian Mapping Authority, Hydrographic Service

**FREEDOM TO CHOOSE** 

## Background



- PRIMAR and ECC have provided support in protection scheme administrator support for S-63 and S-100e4
- PRIMAR PAC 2022 decision to support IHO for S-100e5
- Support since 2003 has covered
  - Development of IHO Scheme Administrator application
  - General training IHO S-63/S-100e4/e5 data protection
  - Scheme Administrator work procedures and operation
  - Ad-hoc IHO SA support (VERY little, basically 2<sup>nd</sup> line)
  - Ad-hoc analyses of scheme participant errors
- Cost covered by PRIMAR Member States
- Development of MoU between IHO and PRIMAR

# Scheme Administrator application

- Functionality
  - Create S-63/S-100 Data Server certificates (.CSR)
  - Digitally sign IHO feature/portrayal/interoperability catalogues compliant with S-100e5.1
    - Creates compressed S-100e5.1 Exchange Set with CATALOG.XML, CATALOG.SIGN and FC/PC/IC file
- Application standards compliance
  - S-63e1.2.1 (Installed looooong time ago)
  - S-100e4.0.0 (further use to be discontinued)
  - S-100e5.1.0 (Installed September 2023)
- Refactored source code to have one application with three configurations (S-63/S-100e4/S-100e5.1)





| IHO SA Application (S-100 edition 5.1) |                      |  |  |             |   |
|--|----------------------|--|--|-------------|---|
| File                                   | Scheme administrator | Data server  | Signature  | Help        |   |
| Data Servers Test77-DS                 |                      | [  | Sign file.<br>Verify Sig   | <br>gnature | 1 |
| Dataserver CSR Subject                 |                      |  | sion: V3<br>ject: CN=urn:mrn:iho:00AA:01810, OU=Test, O=Test I<br>nature Algorithm: SHA256withDSA, OID = 2.16.840.1. |             |   |
|  | 0                    | <pre>Key: Sun DSA Public Key<br/>Parameters:DSA,<br/>p: e103819b 3a5839d8 3cb700a7 01b08095 b74e<br/>cc99454f ec2b87b4 a7d45976 bcb63540 798f5547 3b40f0<br/>4cfc9f9d ef496c40 8553f630 28bf11b8 61d467ff e89021<br/>60a124c9 8fb3fb34 76e04633 59750efd ae59a2c5 8f1912<br/>beb5efc9 ab58f134 7896b668 547a951e 415f0899 288dd0<br/>1df48b7b c20661aa 35170b24 48250a6c 32c564ab 30a7fa<br/>d2c58876 32453cb0 7382b041 f8671fe8 5179c2c7 9edc6e<br/>cf02db0e 9f7f5680 ea9ac5b9 67f869c5 1bb74bc2 7cb2b0<br/>q: 8e7a26bb ef9bb984 d167af6c 5c69dc8a f4bd<br/>g: d378cfad 6c7c441d fdce99f3 2b5023cd 931c<br/>6a555a83 0fa85ca9 b01a552c 8e527619 9f335634 504670<br/>b5e1d117 e3d7d45b 7bd7709b 76f64f28 146c1f42 3df86b<br/>009430a6 33599841 f895f72e 1988d112 6ca9b160 4628f6</pre> |  |             |   |
|  |                      |  |  |             |   |

# **IHO use of Digital Certificates**



- S-100e5.1 IHO Scheme Administrator root certificate
  - Created 09-23 and IHO SA root certificate duration: 2063
  - Only used to create organisational Data Server certificates
  - Identified change to S-100e5 standard
    - DSA q-parameter must be 256 bits
- S-100e5.1 IHO Data Server certificate
  - Only used to digitally sign Feature/Portrayal/Interoperability catalogues
  - IHO Data Server certificate duration: 2063
- Scheme participant certificates duration: 2 years

# **Outstanding Work**



- Additional check that Data Server Certificate Signing Request (.CSR file) has DSA q-parameter = 256 bits
- Update signing functionality for FC/PC/IC catalogues
  - Ensure application creates compliant exchange sets
  - Await consensus on protection encoding in S-164 Test Data
  - Completion November 2023
- Agreed repeat training IHO staff Spring 2024
  - IHO standards, application, procedures