S-164 subWG, M6
3rd August 2023

Agenda

1. Intros (and Apologies)
2. Progress Update and communications
3. Actions and plan update
4. S-164 / S-98 updates
    - Documentation: Papers and Proposals for agreement
    - **Datasets: Update on developments and progress**
5. Breakout meeting summaries
6. **Issues review (from GitHub)**
7. AOB / Next meeting

Progress Update

- Repository
  - Purpose/Process clarified in README (top level) and other README in code tree.
  - S-98 link added to homepage(via Issue)
  - Some S-98 issues added (mirroring those in S-164)
  - Staging Area added(data/Staging)
  - All exchange sets are now in Exchange Sets are (data/ExchangeSets) (process described later)
  - Keys/Certificates added to repo staging area
- Datasets… (coming)

Plan

- Significant dates:
  - NIPWG – September 10-15
  - ENCWG/S101PT – September 25-29
  - S100WG – November XX-YY
  - TSM2024 - tbd
  - HSSC2024 – tbd
- High Level delivery plan in progress. Some issues still require agreement to get final versions drafted. Draft release plan later
- Current plan is to get operational versions to HSSC16 (September 2024)
  - Approval S-100WG (July / August 2024)
  - **Interim major release end December 2023**

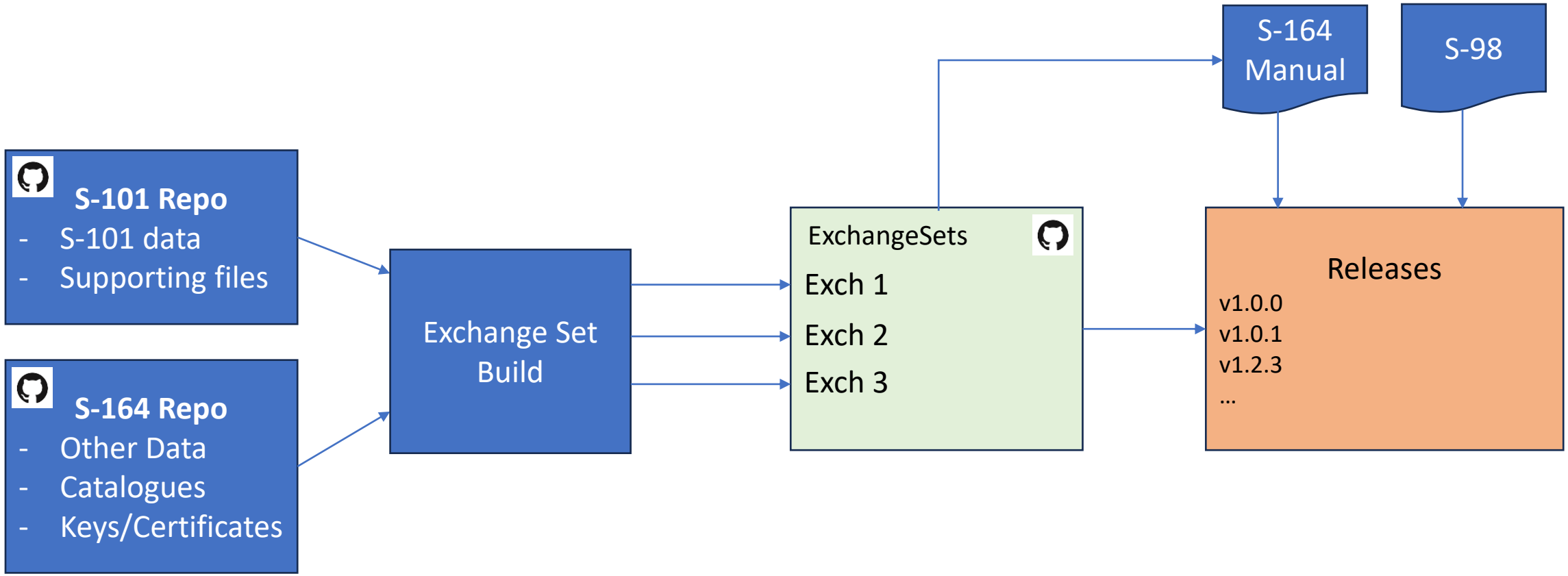
Exchange Sets in progress

- PowerUp
  - New Version in github repository, fixes extents.
- All Initial Catalogues (Sequence of tests)
  - Load Old Catalogues (§2.1.1)
  - Load invalid catalogues (§2.1.2 / §2.1.3)
  - Load incompatible data (§2.1.4)
  - Upgrade Catalogues to new versions (§2.1.5)
  - Load data for both versions + display (§2.1.5)
- Standard Layers - §*(lots!*)
  - Base, Standard and Other cells from S-101-Testdatasets
  - Initial Versions uploaded to GitHub
  - Needs certificates and metadata entries
  - Started reconciling with PC and tests
- Navigational Hazards (x1)
  - NavHazards and Overview cells.
- Dual Fuel
  - SafetyContourDFMon – Safety Contour Dual Fuel cells.
- Polar datasets

Aim is to make these exchange sets release v1.1.0, for ENCWG/S-101PT (includes updated docs)

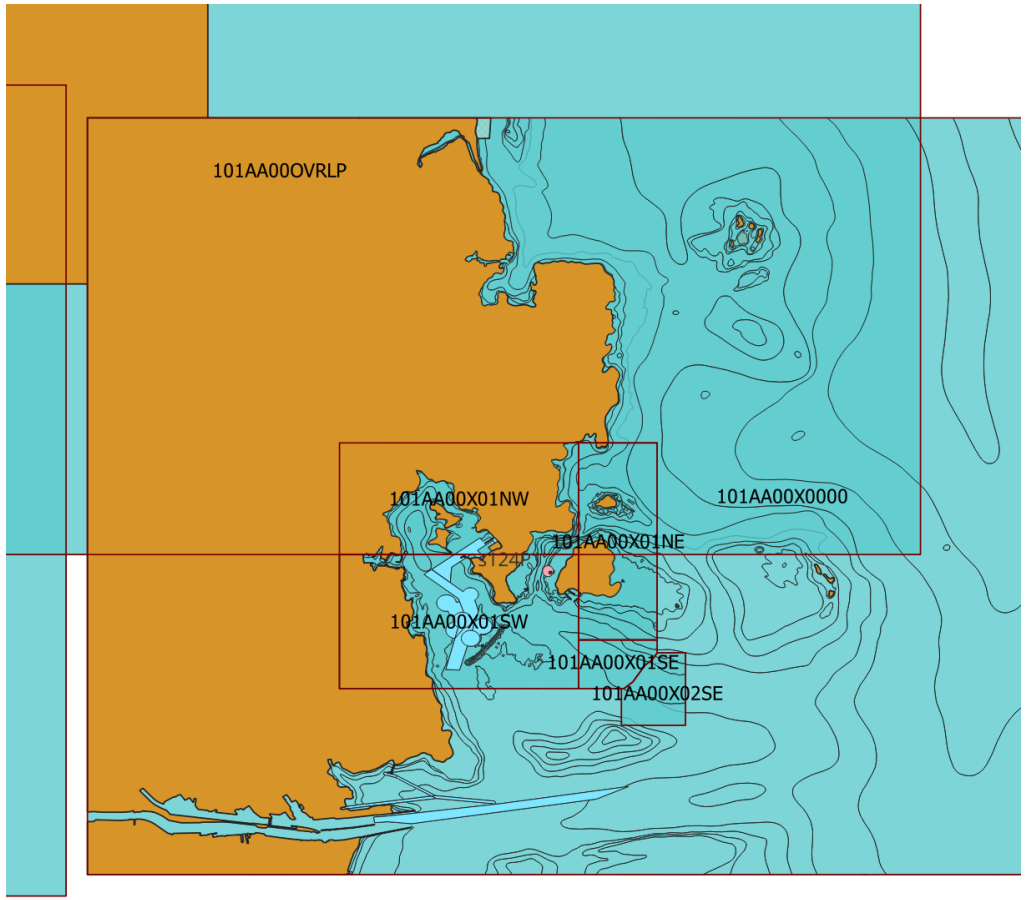
Datasets

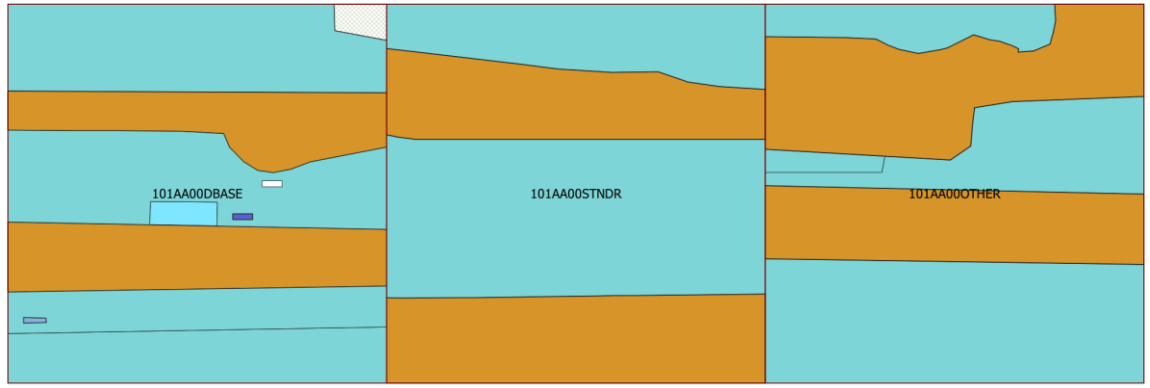
Process for creation.



Release Plan…

- v1
  - Initial Catalogues
  - Std Layers
  - Simple Dual Fuel x1
  - NavHaz x1
  - Polar Data
- v2 (end October)
  - v1.1.0 fixes++
  - Initial version of encrypted/signed data
- v3 (end November)
  - “Chart Display” initial versions
  - Requirements for Data Content complete
- v4 (end December)
  - Navigation Hazards (S-100)
  - Dual Fuel x1





Papers (15 minutes or less)

From last meeting: S164SG5-5

S-164 / S-98 comments and editorial observations

Date:	Document:

1	2	(3)	4	5	(6)	(7)	
Document	**CO[1]**	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the CO[3]**	**Proposed change by the CO**	**Observations** on each comment submitted
S-164_Draft_v1.0.0_TestList.xlsx	SevenCs		Sheet1	ge	Tests for loading encrypted and unencrypted datasets should be rearranged to separate certificate and signature tests from the decryption tests. Justification: For S-100 products, there will be signatures for all datasets (unencrypted/encrypted). Separation of tests will result in a clearer structure and simplify creation of test data.	Insert a section for certificate and signature tests and rearrange to following order: 1) certificate and signature tests, 2) decryption and permit tests, 3) sequence and installation tests.	

No new papers this week. Back next meeting with updates for S-164

Proposed restructuring Section 2

2.6 Loading, Updating and Authentication of encrypted datasets

- Dataset authentication and decryption
  - Certificate and Authentication
    - Installation and management of SA certificate
    - Dataset and exchange set authentication
  - Permit management, dataset decryption
    - Installation and management of permits and datasets
    - Permit expiry

Followed by:

- Dataset Management (multiple data servers etc…)
- Data Services (cancelled/replaced etc..)
- Update Status Report

Keys, Signature, Certificates for datasets

- Currently all datasets are “AA00” producer code (but might become “00AA”?)
- Structure as follows:
  - Cells should be produced and signed by a “producer”
  - Exchange Sets could (should?) be made by an aggregator (RENC?)
  - Exchange Sets could (should?) be signed (CATALOG.SIGN) by an aggregator too, not SA or Data Producer.
  - Top Level certificate is always SA, not included in exchange sets
  - AA00 (producer) != AA00 (scheme administrator), different keys, same organisation.
  - S-128 can also be produced by aggregator keys
- Exchange Sets represent this structure. Example keys/certificates produced.

Keys, Signature, Certificates for datasets

```
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number:
         4c:bb:68:10:8c:14:7b:81:f3:8e:70:9b:b4:a1:6c:b1:ac:80:a6:ce
      Signature Algorithm: dsa_with_SHA256
      Issuer: C = MC, ST = SCHEME_ADMINISTRATOR, O = International Hydrographic Organisation, CN = urn:mrn:iho:org:AA00:1810
      Validity
         Not Before: Jul  3 12:46:54 2023 GMT
         Not After : Nov 18 12:46:54 2050 GMT
      Subject: C = MC, ST = SCHEME_ADMINISTRATOR, O = International Hydrographic Organisation, CN = urn:mrn:iho:org:AA00:1810
      Subject Public Key Info:
         Public Key Algorithm: dsaEncryption
            pub:
               25:bf:ba:69:ff:ef:65:a7:f3:a9:d5:06:92:2a:30:
               bc:02:cb:6e:80:1a:39:76:32:eb:ac:ab:23:d9:83:
               77:3b:0d:95:f6:93:0f:9d:a6:c1:60:5b:2c:8b:65:
               9f:0a:03:8c:51:0a:f0:6d:88:39:a5:47:0a:e0:45:
               0b:11:39:83:8b:ec:85:b5:9d:03:c4:cd:89:cf:db:
               e5:b3:bd:09:17:af:e5:c1:fe:32:23:fa:e0:ae:58:
```

- SA Certificate
- Role=**SCHEME_ADMINSTRATOR**
- Not installed on ECDIS
- Not delivered in Exchange Sets
- Self-Signed by Scheme Administrator (IHO)
- All datasets authenticate against this certificate

Data Producer Certificate
Role=**DATA_PRODUCER**
Installed on ECDIS
Delivered with Exchange Sets

Dataset digital signatures authenticate a dataset against the public key in this certificate and the IHO Scheme Administrator public key

```
Certificate:
   Data:
      Version: 1 (0x0)
      Serial Number:
         70:09:a0:be:98:a2:11:f9:06:82:24:09:80:fc:ab:ed:b2:af:aa:6b
      Signature Algorithm: dsa_with_SHA256
      Issuer: C = MC, ST = SCHEME_ADMINISTRATOR, O = International Hydrographic Organisation, CN = urn:mrn:iho:org:AA00:1810
      Validity
         Not Before: Jul  3 12:49:12 2023 GMT
         Not After : May 11 12:49:12 2033 GMT
      Subject: C = MC, ST = DATA_PRODUCER, O = International Hydrographic Organisation, CN = urn:mrn:iho:org:AA00:1810
      Subject Public Key Info:
         Public Key Algorithm: dsaEncryption
            pub:
               00:94:a3:f8:32:1e:54:13:9d:fe:a2:9d:e5:1c:1c:
               5a:9c:6b:75:7f:9e:01:5d:b9:cb:b7:89:0b:7f:aa:
               b6:1b:74:55:b7:5e:18:1e:8e:8e:a4:0f:76:27:74:
               bd:3e:4e:d5:da:8e:1f:21:3b:91:2b:96:58:25:9f:
               73:4b:fe:e6:73:29:ad:13:79:9a:79:f6:40:ee:2a:
               0b:d3:29:08:42:4f:99:9d:5c:48:ac:73:ec:3e:a9:
               1b:f1:7d:ea:66:39:12:48:66:ba:84:b9:9b:ad:ab:
               e9:38:1a:ea:9e:52:4b:fe:4f:33:fa:50:56:5e:5c:
```

Breakout meetings

- Updates to S-164/S-98 (and S-52) for Quality Objects/Features in Dual Fuel ECDIS – Mtg 1 held. Paper for ENCWG (September)
- Water Level Adjustment – End August
- Manual Editing / Manual Update – Early September
- NIPWG (UI for NPUBS) – Initial meeting held. Paper to go to NIPWG (September)
- S-100WG for “WLA 2” – how to integrate WLA into S-100 GFM/Portrayal engine. tbd but an initial meeting will feed into S-100WG in November.

Github – Some focused Issues to think about.

- **Version mapping between catalogues and datasets./Display of S-101 ENCs with different FCs and PCs**
- **Unofficial vs Official Data / Signature and Certificate formats and content**
- **Content of CATALOG.XML / Service Elements creation.**

AOB

- Any other business (All)?
- Next meeting?
  - Between NIPWG and ENCWG/S-101PT
  - Focus on datasets and outputs from breakout meetings