

**Paper for Consideration by S-100WG****Governance of Catalogue distribution**

<b>Submitted by:</b>	IIC Technologies / S-164 sub working group
<b>Executive Summary:</b>	A formalised, inclusive, safe distribution process for catalogues is required
<b>Related Documents:</b>	S-100
<b>Related Projects:</b>	S-100 data protection scheme

**Introduction / Background**

An issue raised in the S-164/S-98 subgroup has focused on a topic raised previously in the S-100 Governance Document, namely the governance process surrounding the distribution of S-100 catalogues (Feature, Portrayal, Interoperability) by the IHO Secretariat. These catalogues, XML based, are complex documents and currently no formalised structure exists for their review and subsequent distribution and use by end users. Given the dire consequences of their misuse, corruption or incorrect content a more structured, inclusive and rigorous approach to the distribution and authoring process is recommended for implementation of “live” catalogues. An initial process, for discussion and development by the IHO secretariat, working groups and the S-100 community is contained in this paper.

**Analysis/Discussion**

Currently there are a number of bodies in the IHO community building feature/portrayal and interoperability catalogues and the number of discrete tools available for their creation is similarly growing. Catalogues all must conform to an XML Schema, defined within the (current at the time) S-100 Schemas. Most groups utilise software tools for the creation of feature catalogues (in the vast majority of cases, they are derived manually from the UML models forming the application schema) and project teams similarly develop and validate portrayal catalogues according to their requirements. Validation against schemas, however, are not infallible against inconsistencies and incompatibilities with other product specifications, nor against a number of other issues that they may have.

In most project teams S-100 PT members then review catalogues alongside product specification details, and some (S-101 notably) review catalogues as a specific milestone, prior to their broader release.

An additional observation worthy of note (and brought up in recent meetings) is the inclusion of a fully featured programming language in the portrayal catalogue structure, Lua. Such a mechanism, if misused, poses a serious cyber security risk and this requires management and mitigation measures.

Industry representatives have registered concerns that catalogue distribution (and attendant rigorous processes for ensuring their correctness) is currently undefined other than a standard release process for product specifications. They have asked for a broader debate within the IHO working groups to see if a more rigorous process can be established prior to go-live of any S-100 product specifications. The impacts of corrupted or incorrect catalogues could be significant, particularly in the context of portrayal catalogues (for the reason outlined in the previous paragraph).

Governance should involve, as a minimum:

- A better defined process for release of catalogues for operational use
- The involvement of implementers to enable issues to be found.
- Defined, rigorous validation tests across all catalogue elements prior to any operational distribution
- Extending use of digital signatures to ensure integrity during assurance and testing processes

A proposed process for catalogue management covering the period between its definition by the project team responsible, and its operational use is proposed thus:

1. Project Team drafts product specification and catalogues (with optional inclusion in interoperability catalogue)
2. Internal review of catalogues by project team to ensure they match the objectives of the product specification and match the Application Schema.
3. A new validation Phase: This should include rigorous, external (to the PT) independent validation
  - a. Against current S-100 schemas
  - b. Using specific validation tests defined at the S-100 level.
  - c. Once passed, catalogues are digitally signed by the IHO acting as a data producer and labelled with a status (in the signature certificate) of "DRAFT". Certificates are valid for the review period only.
  - d. Passed to broader groups consisting of:
    - i. Nominated technical experts at the S-100 level
    - ii. OEMs registered with the data protection scheme
    - iii. RENCs and distributors registered as AGGREGATORS under the security scheme
    - iv. Test data must be included with catalogues distributed including:
      1. Valid, representative data for the product specification
      2. "Chart 1" style portrayal
      3. Exhaustive test data for non-trivial Lua scripts.
    - v. If included in an IC then test data to allow full testing of IC shall also be included (who produces this? S-98 team? An S-98 permanent subgroup of S100WG?)
  - e. Period of review to be established.
  - f. There should be an opportunity for review, comment and modification should it be necessary. OEMs are able to do testing and feed back to IHO and PT members, raised issues can be addressed and arbitrated by S100WG if necessary
  - g. Such a review is iterative and new draft versions/data may be posted to help representatives as much as possible. Consensus must be achieved by all stakeholders prior to release for operational use.
  - h. Once agreed, catalogues are considered live, they are re-signed by the IHO, verified as identical and given certificates with a long lifespan (e.g. 10 yrs), marked with a status of "LIVE". These are the **only** catalogues which may be installed on ECDIS and catalogues and signed by the scheme administrator acting as a data producer (as identified in the role in the certificates). Others should be excluded (and the process documented in S-98 Annex C).
4. Distribution of "Live" catalogues:
  - a. Once live, catalogues can be distributed by any party – there is no obligation on aggregators nor data producers to distribute to end users – defining the channel to the user is not the function of the IHO but thought and space should be given for evolving rigorous delivery mechanisms which can be used from S-100 "go-live" (maybe via the S-100 infrastructure task teams).
  - b. If OEMs wish to distribute directly to their customers they may wish to do so, supplementing it with engineering support but it is acknowledged this is not the only model. Certainly it should be impossible to install unless signed by scheme administrator acting in the role of data producer (this should be added to S-98 under catalogue installation).
5. The IHO website will contain wording on how to differentiate test/draft from operational catalogues and how to verify digital signatures and understand the certificate fields for the stakeholder groups.

## Conclusions

The S-100 catalogue mechanisms are powerful and rich in functionality. There are currently few processes for independent review, testing and validation which reach all stakeholders and consideration should be given to this aspect of the "operationalisation" of S-100 prior to go-live of product specifications and data services.

## Action Required of S-100WG

### S-100WG is asked to:

1. Consider the observations made in this paper.

2. Work with IHO secretariat and working groups to develop and adopt a post-publication process for final approval/distribution of catalogues for product specifications used in ECDIS
3. Identify or establish a permanent group responsible for dealing with inter-product catalogues (interoperability) and for oversight of distribution testing and processes.
4. Ensure suitable tests exist in S-164 for installation and identification of expired certificates.
5. Inform existing OEMs of new arrangements and add external consultation to new agreements.
6. Build wording which can be included in IHO website explaining processes to new participants in the S-100 community. Establish communications through dedicated email addresses for queries and issues