Progress report – S-63 migration to S-100 Part 13

A small group met in Genoa in March 2017 during the S-100WG meeting to discuss the passage of the existing IHO S-63 content into S-100. This group comprised:

1. Jonathan Pritchard (Chair)
2. Hannu Pieponnen (IEC, Furuno)
3. Julia Powell (S-100WG, NOAA)
4. Robert Sandvik (ECC)
5. Konstantin Ivanov (Transas)
6. Bob Greer (Spawar)
7. Mikan Stamenkovich (Spawar)
8. Tony Pharaoh (IHB)

A summary discussion was held around various aspects of the existing S-63 standard and operation of the IHO data protection scheme. At this meeting JP agreed to send out the current iteration of the draft S-100 part. This has been done and feedback asked for.

The March meeting concluded four main areas where edits were still required in the draft document:

1. A general tidying up of content. This also requires expansion to some parts where the description is incomplete.
2. File Format tables and example data. The tables which define the individual elements of the standard (e.g public / private keys, SSK, signed Public Key) need completion and comprehensive base64 encoded examples producing to complete the chapter.
3. Service elements to be added. The service elements were previously taken out and delegated to the individual product specification. There was a request to put the service elements back in S-100, albeit at a conceptual level within S-100 leaving the individual product specifications to customise a basic model of updated/revised datasets. This allows S-101 to implement a "service.xml" file and allows other product specifications to implement similar specs based on the nature of the data they have.
4. Multiple Certification Authorities should be implemented allowing for multiple scheme administrators who can verify identity within domains other than the IHOs. Although only one SA currently exists (the IHO) conceivably others such as IALA, e-Nav authorities etc could also act in the role as scheme administrator, verifying identities of scheme participants.

Progress so far:

Some progress has been made on these areas since the Genoa meeting.

- A new subsection defining service elements has been drafted and updates to the tables on file formats is nearly complete.
- Some progress has been made tidying up the existing content, particularly the tables containing the specifications of public/private keys and signatures.
- I have reworded the existing draft to account for multiple scheme administrators in line with the meeting outputs from Genoa. This actually is not such a difficult task. The main difference is the description of the individual SAs (they will need to have identities just like

anyone else.) – There is a need to discuss how, practically, this can be implemented but as far as S-100 is concerned the role can just be defined and left to the participating organisation to implement. There are some details to be worked out here (mainly, how implementing systems authenticate against multiple potential SAs and whether a data server needs to have an "owning" SA to show which one authenticates it) but I believe these can be worked out by correspondence once the part is drafted.

- I will issue a revised version of the document to the group participants by the end of the month (September) and then will ask for a more formal review of the new part with a view to its completion at the end of December – this is to provide input for the main S-100WG meeting in 2018.

In addition to the core document updates the following actions have been identified:

- Changes to S-101 to define the service elements required by ENC/ECDIS systems. This will effectively be a definition of a file (currently called service.xml) which replicates the function and content of the existing PRODUCTS.TXT and SERIAL.ENC files in the S-57 version of S-63. The new section of S-100 will specify the content and functionality required by service elements leaving S-101 to supply a normative definition of the files required.
- S-101 will also need to contain the equivalent of the ENC status report (As currently implemented in S-63).
- A final definition for S-100 (and S-101) for catalogue metadata fields relating to data compression, encryption and digital signatures.

I am still struggling to find member states and contributors to the new S-100 part. If anyone wishes to be involved they should contact me at :

Jonathan.pritchard@ukho.gov.uk or visit the google group at:
https://groups.google.com/forum/#!forum/s63dev

Jonathan Pritchard,
United Kingdom Hydrographic Office,
Taunton, UK