A few quick notes on S-63 / S-100 for the meeting Monday 18th June.

I’ve done a quick readthrough of the document supplied by Robert and a few observations are below:

1. Change of algorithm. There’s a proposed change of core encryption algorithm to AES. This needs some discussion. In the past (largely motivated by OEMs) there was a desire to retain Blowfish as the encryption algorithm to minimise the need for rework. This should be considered further – I’m not aware of any particular issues with Blowfish itself and whilst I agree the key lengths need to be lengthened to reflect current best practice a change of algorithm would be a big change.
2. Multiple SAs. At the meeting in Italy it was requested that we adopt a multiple-SA configuration for the scheme which would map to each of the registry domain controllers. I believe the idea was that each SA would be independent and control its own entities and identities. This is similar to e.g multiple root certificates in browsers and the IHO would need to host the self-signed root certificates as a central point of reference.
3. Permit formats seem to be unchanged from the text format defined in S-63. Previously we’ve adopted an XML approach to the permits and integrated a base64 signature into them. Need to agree this – the system in the doc works but we should debate the technical pros and cons.
4. Separate signature files. One of the early plans in the revised version was to embed the signatures of each dataset file in the catalogue metadata file. This avoids the need for separate signature files for every single dataset file (which double the number of dataset files and imposes a folder-specific dependency on any implementing systems).
5. There’s no digital signature format specified. The position within the existing draft is to use base64 encoding and then embed the textual format of the digital signature in the catalogue metadata. This means the signature is not subject to differences of encoding (e.g line feed/carriage returns which plagued the existing format) and means they can be embedded without issues. This needs debate. I’m happy for signatures of permits to be separate files if required (as there’s only one per permit) but separate for every file in the dataset seems against the spirit of S-100 to me – we were trying to integrate the elements of s-63 into S-100 (this also means a digitalsignature can replace CRC32 in some product specifications if necessary)
6. We need to make sure the document (which will be a part of S-100) makes it clear which parts are S-100, which parts are specific to S-101 and which parts are guidance to implementers of other S-10x products
7. I believe we do need to retain “service level” elements (i.e an updated version of products.txt) as for S-101 these are still necessary to provide the implementing system with information about the revision of data within the service (which aren’t necessarily contained within the exchange set) – they can be simplified (and we talked a lot of about service.xml instead of products.txt etc…) We have some words drafted on this already within my revision.
8. There’s a need to make sure signatures and copy protection elements are separable. Some member states want to implement digital signatures without copy protection and the scheme needs to reflect that requirement, potentially for multiple products. This shouldn’t be difficult and should be defined within the catalogue metadata (again, helpful if the signatures are contained within the catalogue).
9. Other elements we need to consider – test data creation, status message (SSE etc), media layout, ECDIS status report.