Part 15

Part 15 revision Overview.

Result of intercessional discussions between Part 15 stakeholders, producers, industry and aggregators.

Overview

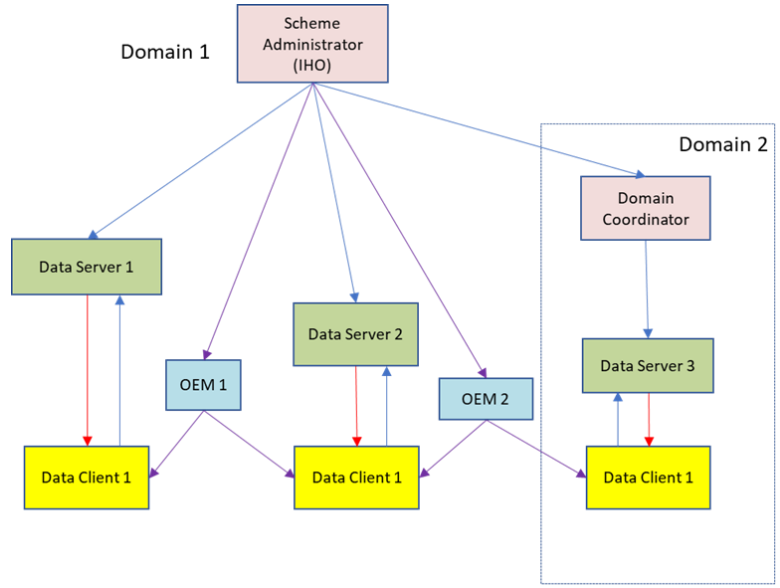
1. Updated, complete list of referenced standards, including X.509, ASN.1 and AES.
2. Better specifications of scheme participants, especially domain coordinators, their roles and responsibilities
3. Corrected diagrams showing interaction of scheme participants and the information exchanged between them.
4. Defined XML content against schemas covering digital signatures and permits including descriptions of the various defined fields for all implementations in the catalogue metadata, permit files and their digital signature files.
5. Integration of digital signature content with proposals put forward for exchange set creation and metadata.

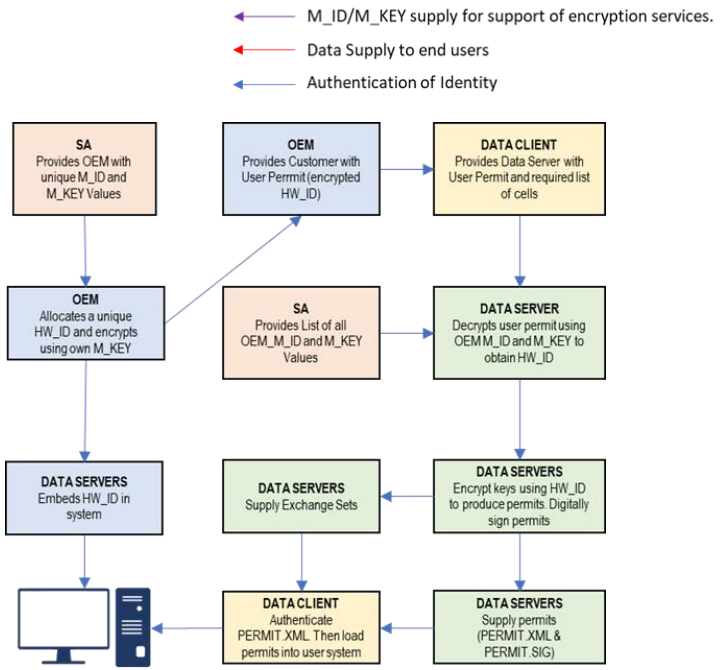
Also:

1. Increase of key length for SA root key to 2048 bits
2. Added algorithms to enumeration to future-proof and for better interoperability with external standards (eNav)
3. Items required by metadata, Part 17 URNs for locating supporting resources via digital signatures and checksums

Revision to Part 15

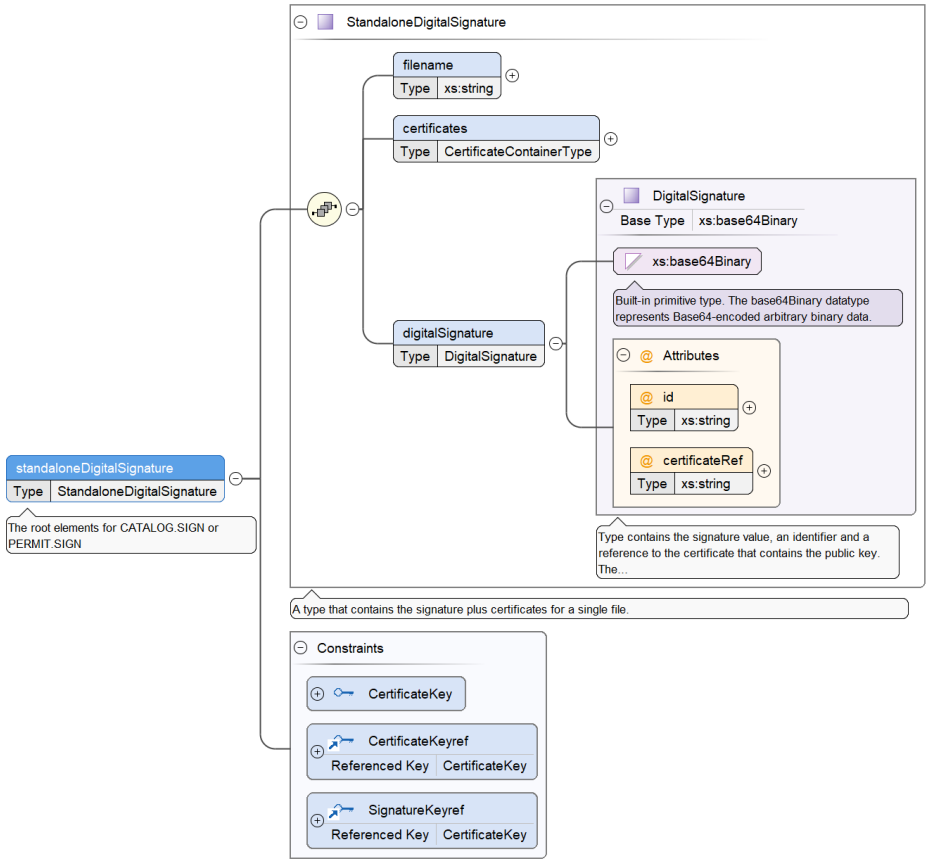
- Clarification of purpose – file based transfer of S-100 data
- Clarification of Scheme Participants – Clarify definition and roles of “Domain Coordinators”, also included in diagrams
- Corrections to existing diagrams including old S-63/S-57 items
- Corrections to values in examples, also corrections to XML and harmonisation with proposed XML Schemas





Proposals for Part 17 support

- Multiple Digital Signatures are supported, minimum is 1
- Names and definitions clarified
- Proposed XSD for Part 15 support include
  - Standalone validatable and reusable schemas for PERMIT.XML, PERMIT.SIGN and CATALOG.SIGN
  - Defines types, structure and multiplicities
  - Certificates held in header of CATALOG.XML
  - id and reference tie signatures to certificates in CATALOG.XML. Certificates identified by issuer.
  - >=1 digital signatures for all resources (signature + additional). Signatures can be on unencrypted, compressed archives or encrypted.



Revisions to Part 15

S-100 Digital Signature MRN		
Name	**Value**	**Example**
Prefix	urn:mrn:iho:s100:dsig	
Algorithm	From digitalSignatureReference (Part XX 4a-5)	dsa
Value	Computed digital Signature value	302C021421EF1102A1BA0416FC6A8F916114FBB991F94A2E02146C4D87E83D4AEEBC15AC23B2A6F2A7301A681A7C
Example	urn:mrn:iho:s100:dsig:dsa:302C021421EF1102A1BA0416FC6A8F916114FBB991F94A2E02146C4D87E83D4AEEBC15AC23B2A6F2A7301A681A7C	

S-100 Cryptographic hash MRN		
Name	Value	Example
Prefix	urn:mrn:iho:s100:hash	
Algorithm	digitalSignatureReference (Part XX 4a-4.5)	sha256
Value	Computed cryptographic hash expressed as hexadecimal	a948904f2f0f479b8f8197694b30184b0d2ed1c1cd2a1ec0fb85d299a192a447
Example	urn:mrn:iho:s100:hash:sha256:a948904f2f0f479b8f8197694b30184b0d2ed1c1cd2a1ec0fb85d299a192a447	

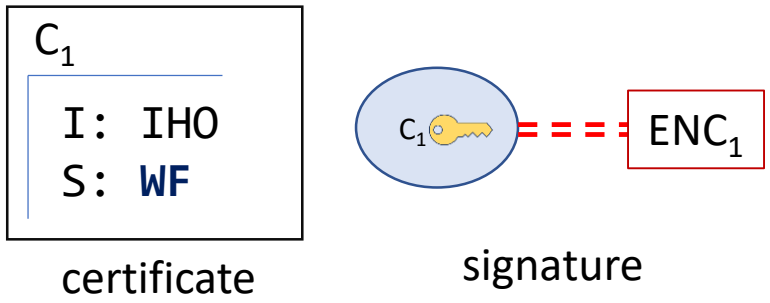
- Signatures are Base 64 encoded. Unambiguous and shorter
- Tightened up how Signatures link up to certificates and identification of root certificates, illustrated with examples from Schemas
- Proposals for MRNs to represent signatures and checksums

```
<digitalSignatureValue>
 MEQCIHVvkGrJl0joEqmS5PCmnJW4pydisZW5gpJGoU3CUeOVAiAZvuRA0y3QDLgnzJ8Il4oFX4U40BJ36UhRBVLUFfiVwQ==
</digitalSignatureValue>
```

Other Items / Impacts

- Proposal for establishing working procedures for the data protection scheme. This could also define a TR for the algorithms used
- Should also clarify the relationship between “data producer” as defined by S-62/register of data producers and Organisation within the X.509 certificates which authorise digital signatures
- Doesn’t affect Part 15, just clarifies how it is used to support S-100 ECDIS and how (if needed) legacy S-63 support is implemented alongside.
- S-98 Annex C
  - SSE Codes, Update Status reports and flowcharts from S-63 have been migrated to S-98 Annex C
  - Governance / “What Overlays What?” – Part 15 could be used as a mechanism for determining which S-XXX products are able to overlay S-101/S-401 (“ENC”)

```
Certificate:
   Data:
      Version: 1 (0x0)
      Serial Number:
         ef:94:94:9e:f9:e5:68:9c
   Signature Algorithm: dsa_with_SHA256
      Issuer: C=MC, ST=Monaco, O=International Hydrographic
Organization, CN=IHO Data PRotection Scheme Adminstrator
      Validity
         Not Before: Dec  4 07:29:39 2021 GMT
         Not After : Jan  3 07:29:39 2022 GMT
      Subject: C=UK, ST=Some-State, O=Internet Widgits Pty
Ltd, CN=Data Server Test 1
      Subject Public Key Info:
         Public Key Algorithm: dsaEncryption
            pub:
               57:25:6b:42:6c:c5:42:ab:53:b7:bb:cd:df:12:b0:
               45:2f:50:5d:c2:7d:70:1d:65:83:9d:24:0b:42:1b:
               49:fb:cb:f0:c3:7c:52:30:eb:e0:11:cb:27:6c:ff:
               b5:92:c2:c4:60:1e:2b:ed:d8:d9:92:40:75:de:1f:
               49:22:c8:cf:d6:e1:c0:bf:67:71:25:f7:dc:c3:7f:
               84:9a:02:a5:d9:48:85:76:51:0f:95:5a:80:bf:ee:
               17:be:e3:62:8d:30:42:e2:5c:24:b9:c6:5d:fa:68:
```



The S-100 working group is asked to:

- Review and comment on the content of the revised Part 15 of S-100
- Approve the creation/finishing of specific schemas representing the XML content of Part 15
- Approve the creation of an IHO Technical Resolution detailing the algorithms used by S-100 for data protection and authentication
- Approve the creation of procedural documentation by IHO Secretariat, member states and industry participants covering the details of the implementation of the IHO security scheme under S-100 using the proposed content in this paper as a guide.