S100WG6 -4.22

Paper for Consideration by S-100WG

Revision of Part 15

Submitted by:	UKHO, IIC
Executive Summary:	Revision of S-100 Part 15
Related Documents:	S-100 Edition 5.0.0
Related Projects:	

Introduction / Background

A revision to IHO S-100 Part 15, the data protection scheme has been drafted. The revision clarifies certain aspects of Part 15 and its implementation, corrects factual and typographical errors and expands key sections which were under-described in edition 4.0.0

Analysis/Discussion

Part 15 of S-100 has been revised to take into account comments received during the lifetime of edition 4.0.0 and to clarify several sections where the standard is ambiguous and/or incorrect.

Summarised, these clarifications consist of:

1. Updated, complete list of referenced standards, including X.509, Base 64, ASN.1 and AES.
2. Better specifications of scheme participants, especially domain coordinators, their roles and responsibilities
3. Clearer diagrams showing interaction of scheme participants and the information exchanged between them.
4. Corrections to examples and several contradictory areas of specification
5. Enhanced XML schemas content covering standalone and embedded digital signatures and permits. This includes descriptions of the defined fields for all implementations in the catalogue metadata, permit files and their digital signature files.
6. Integration of digital signature content with proposals put forward for exchange set creation and metadata. This includes specification of MRN namespaces for digital signature and hash values.
7. An increase of the SA key length to 2048 bits.

Procedural documentation.

The current IHO data protection scheme under S-63 has been in operation for nearly twenty years. In that time the number of participants has grown dramatically and the IHO secretariat has gained a lot of experience in various aspects of its operation and how the various elements should be organised.

No governing documentation yet exists specifying how the scheme as a whole should be operated and the new S-100 Part 15 now focuses solely on the technical details of its implementation. An additional challenge during the implementation phase of S-100 will be the maintenance of the existing S-57/S-63 based data protection scheme alongside the rollout of the S-100 elements of the scheme. S-100 Part 15 is similar in its layout to S-63 but several significant differences exist, namely:

1. Differences in key lengths for some of the algorithms
2. The introduction of AES encryption
3. Domain Coordinators
4. A clearer separation between data protection and authentication
5. A focus on the technical details of data protection. Many elements of S-63 have been relocated to other areas of the S-100 parts and S-98 Annex C.

Recommendations

This covering paper proposes both the creation of an IHO technical resolution defining the specific algorithms and key lengths used within Part 15 for transfer of file based S-100 product specifications to S-100 ECDIS under IHO standards, and also the creation of detailed procedures for the administration of the IHOs entire data protection scheme and its participants.

These procedures should cover, for the entirety of the data protection scheme:

1. Application processes for prospective members of the scheme.
2. Responsibilities of the scheme participants and specification of the roles each participant is able to be assigned to.
3. How participants' roles, users, organisations and domains are embedded in the X-509 fields used by S-100 Part 15.
4. Details of the day to day initiation and operation of the scheme for both S-57/S-63 and S-100 elements.
5. The role of domain coordinators and which roles are delegated to them.
6. Maintenance of record by data servers.
7. Distribution of M_ID/M_KEY material

Justification and Impacts

The introduction of the S-100 Part 15 elements of the data protection scheme are arguably more complex to effect than the initial introduction and evolution of the S-63-based scheme. The development of a detailed plan and procedures by scheme stakeholders will efficiently define how the scheme will operate as S-100 ECDIS is developed and the initial S-100 product specifications go live.

The revisions to Part 15 will clarify how various elements operate and data is exchanged throughout the IHO ecosystem.

Action Required of S-100WG

The S-100 working group is asked to:

1. Review and comment on the content of the revised Part 15 of S-100
2. Approve the enhancements to the schemas representing the XML content of Part 15
3. Approve the creation of an IHO Technical Resolution detailing the algorithms used by S-100 for data protection and authentication
4. 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.