**S100WGXX xx-xx**

## Paper for Consideration by S-100WG

## Revision of Part 15

|  |  |
| --- | --- |
| ***Submitted by:*** | IIC, Maritime Connectivity Platform |
| ***Executive Summary:*** | Revision of S-100 Part 15 |
| ***Related Documents:*** | S-100 Edition 5.0.0 |
| ***Related Projects:*** | IALA G1128 |
|  |  |

## 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. Discussion with bodies external to IHO, who are developing compatibility with S-100 ECDIS under other IEC proposed standards have been consulted and provided feedback on the revision.

## Analysis/Discussion

Part 15 of S-100 has been revised to take into account comments received during the lifetime of edition 4.0.0. Additional proposals have been received from IALA E-Navigation representatives and reflect an alignment of S-100 with broader IEC standards, most notably SECOM (IEC63173). These are listed below:

Summarised, these clarifications are:

1. A recommendation to increase the key length of the Scheme Administrator’s key to 2048 bits from 1024 bits
2. A request to add additional digital signature algorithms to S-100’s digitalSignature enumeration in S-100 metadata.

Taking these recommendations individually:

**Increase in key length.** The current key length in S-100 is 1024 bits and this is stated early in Part 15. Amongst various working groups (not just in maritime data systems) the trend is for longer key lengths to future protect systems. The current record for factoring (i.e. breaking) such keys is 829 bits (set in early 2020). Additionally leading certification authorities including Verisign and ICANN (Internet Corporation for Assigned Names and Numbers) have signalled since the mid 2010s the move away from 1024 bit keys for SSL certificates. Verisign themselves have switched to 2048 bits and no longer accept 1024 bit certificate signing requests.

Whilst wholesale vulnerabilities in keys of 1024 bits is likely to be some way off, it should be borne in mind that the provisions of S-100 Part 15 may have a considerable lifetime and the task of updating the IHO’s SA key are onerous. The shift to 2048 requires an issuing of the IHO’s SA key and updates to keys of the entities it certifies. At this stage, given that no live S-100 data is being used in S-100 ECDIS the impact is minimal. If, 7-8 years from the time of writing 1024 keys are factored the impact would be both costly and time-consuming.

**Extra algorithm specifications**: The following are requested in the enumeration of S-100 digitalSignature to allow greater expressivilty in S-100 CATALOG.XML metadata specification of digital signature and encryption algorithms.

* 1. [RSA] RSA with key length >= 2048 bits,
  2. [DSA] DSA with key length >= 2048 bits,
  3. [ECDSA] ECDSA with key length >= 224 bits.
  4. [ECDSA-224-SHA2-224] 224 bits ECDSA with SHA2-224 hashing
  5. [ECDSA-224-SHA3-224] 224 bits ECDSA with SHA3-224 hashing
  6. [ECDSA-256-SHA2-256] 256 bits ECDSA: SHA2-256
  7. [ECDSA-256-SHA3-256] 256 bits ECDSA: SHA3-256
  8. [ECDSA-384-SHA2] 384 bits ECDSA: SHA2-384
  9. [ECDSA-384-SHA3] 384 bits ECDSA: SHA3-384
  10. [AES-128] – AES 128 bit keys
  11. [AES-192] – AES 192 bit keys
  12. [AES-256] – AES 256 bit keys

The IHO community has expressed the desire to standardise on a single encryption algorithm for file-based transfer of S-100 data such as S-101 and other S-1XX data standards and this proposal does not impact that desire.

In order to achieve better interoperability with other standards which may be implemented on vessel based systems the proposal is to add these enumerations to the S-100 digitalSignature metadata to enable exchange set metadata to describe them. This could also extend to negotiation of data across future API data exchange. Separately, a proposal has been made for the IHO to establish procedural documentation governing the operation of the data protection scheme and it is recommended that use of alternative algorithms is covered there as well.

## Recommendations

This paper recommends the increase of the DSA keys used for the SA root key to 2048 bits to future-proof implementation of Part 15 and the documentation of this increase in S-100 Part 15 and/or the IHOs procedural documentation.

## Justification and Impacts

The impact of increasing the key length of the IHO SA Key length is, as stated, small in comparison to the impact of changing it within the timeframe of the decade of implementation. The impacts are:

1. The IHO would have to reissue data server certificates for current S-100 enrolled data servers and use them on an ongoing basis
2. The length of data server certificates would double. These are included only once in S-100 dataset metadata though which minimises the increase in metadata size. Signatures themselves would also increase in length but such an increase is manageable as the size of signature text in CATALOG.XML is small compared to other content and prudent given the increase in security and alignment with mainstream data security bodies it affords.

The impact of allowing extra specifications for signature/encryption algorithms should be nil for S-1XX development and implementation on ECDIS. The extension of such fields increases interoperability of S-100 Part 15 with external standards in development.

## Action Required of S-100WG

The S-100 working group is asked to:

1. Review and comment on the contents of the paper provided
2. Approve the increase of the SA key length to 2048 bits
3. Approve the inclusion of extra algorithm specifications in S-100 exchange set metadata.
4. Approve modifications to Part 15 contents and exchange set schemas in respect of the proposals.