Paper for Consideration by S-100WG

Productionising Part 15 – Identifiers and procedures

Submitted by:	IIC Technologies,
Executive Summary:	Productionising S-100 Part 15
Related Documents:	S-100 Part 15 / S-100 Part 17
Related Projects:	IHO Data Protection Scheme

Introduction / Background

S-100 Part 15 has gone through a significant revision in edition 5.0.0. As part of an implementation at S-100WG7 a decision was taken to establish working procedures for the operation of the scheme by the Schema Administrator, the IHO Secretariat. This paper introduces a number of items relevant to development of those procedures in anticipation of the launch of the Data Protection Scheme under Edition 5.0.0.

It is also hoped that together observations and recommendations will assist data producers, aggregators/distributors and ECDIS OEM implementers in the coming weeks and months, as S-100 Edition 5.0.0 becomes operational.

Analysis/Discussion

The increase in key length to 2948 bytes which was introduced in edition 5.0.0 must be implemented by the SA. This means a complete reissue of the SA public key certificate as well as new certificates for all data servers which are signed by the new SA certificate (and re-submitting of their certificate signing requests to comply with the new key length).

At this stage expiry dates for data server certificates can be set. These should probably be harmonised with appropriate dates defined by the Scheme Administrator. Whilst the SA certificate should have a long date spanning S-100 ECDIS (30 years, say) each certificate issues should have a shorter expiry date due to the lack of formal revocation procedures. Certificates can be included in exchange sets under S-100 Part 17 and so can be reissued alongside data by distributurs without issue (as long as such test cases are added to S-164). This defines the IHO formal revocation procedures for the ECDIS use case.

The proposal in this paper is that the reissue of the data server certificates is also used as an opportunity to standardise some of the fields in the certificates for the purpose of clarity.

The current S-62 concept assigns a numeric and character code to each data producing “entity” within the IHO. There is a one-many relationship between the member states and their producing organisations. It is recommended that these identifiers defined in the producer registry are used as common name identifiers in the digital certificates issued by the IHO SA, certifying their identity. Using the S-100 convention of MRNs (in line with other similar organisations such as MCP) the S-62 codes can be embedded in each data server certificate.

The reason for this is partly to standardise the free text fields in the certificates, and partly to link the identity being certified with the entity producing the data. In the current regime there is no machine readable standardised link between the digital signature identity and the data producer.

In the current regime data can be digitally signed and the end user knows it is complete but not “who” has produced the digital signature, e.g. I can apply for a digital certificate where the name field contains the string “IIC Technologies acting on behalf of NOAA” even though I have no formal permission to sign data on behalf of NOAA..

This process of standardisation also deals with any updates to the producer code registry at the ECDIS as IHO certified identities can then be linked to data which is issued by new/amended producers.

In this scheme the proposal is for the X.509 certificates (defined under S-100 Part 15) to contain the following content in the fields customisable by the certificate requester. A full diagram of the certificate issued by the SA is contained in Annex A

The following values are proposed:

- C (Country) = **ISO Country Code of state making request**
- ST (State or Province) = **A code reflecting the role of the subject**
- O (Organisation) = **member state organisation name (text)**
- CN (Common Name) = **IHO data producer code integer and alpha code (as part of a colon separated MRN), e.g. urn:mrn:iho:aa:1810 or urn:mrn:iho:GB:540.**

These fields are implemented by the data server who applies for a certificate, and by the IHO when certificates are generated. The proposal is for the IHO Secretariat, acting as the scheme administrator to enforce the format of these fields when certificate signing requests are received.

Justification

1. These fields are required by the X.509 format but are currently structured text
2. It makes sense to classify certificates by the "role" of the subject, and to link their IHO "identity" to the identity defined in the certificate.
3. There is currently no way of establishing whether a certificate certifies an IHO data producer or another role under the IHO

Distribution of Catalogues by IHO secretariat

Part of the IHO role in the S-100 rollout will be to provide feature, portrayal and interoperability catalogues for use by ECDIS end users and others. It is proposed that, in accordance with Part 17, these catalogues are always distributed with an accompanying CATALOG.XML and IHO digital signature. This gives end users the absolute assurance that the catalogue content is complete and issued by the IHO. This element should be clarified in S-98 Annex C (or Part 17 itself). This implies that the SA must have a facility for production of digital signatures and conformant CATALOG.XML content to support the users of the data protection scheme. Such catalogues can be imported directly into CATALOG.XML produced by aggregators and service providers as necessary fro distribution to end users. The IHO will have its own identity within the scheme (the "AA" producer code")

Ultimately the structures under Part 15 provide clarity to end users of the identity of data issuers, aggregators and producers using a simple, flexible, extensible scheme. The time to implement this structure should be at the commencement of the S-100 edition 5.0.0 data protection scheme.

Establishment of a "landing page" for the data protection scheme

Following on from the recommendation made at the last S-101PT, part of the rollout of the data protection scheme should be a landing page to serve as the central resource. This should contain information on how to generate keys and CSRs, including the formatting of the fields which are required.

Revocation procedures

The scheme has no formal revocation procedures, relying on expiration of certificates. This should be examined in more detail but, due to the ECDIS environment is unlikely to be possible within the current structure of the scheme. As discussed in the first section of this paper, revocation can be partly dealt with by having appropriate certificate expiration dates issued by the SA to participants.

Implementation details.

Obviously, at some point the IHO secretariat will consider the status of the S-100 Data protection scheme as "operational" for edition 5.0.0 – the question of how to manage those participants who have already implemented edition 4.0.0 Part 15 should then be considered.

The recommendation would be to require new registration for those participants who require certificates, in order that the identity identifiers can be standardised and for agreements to be put in place. OEM M_ID/M_KEY pairs are unchanged under edition 5.0.0 but, as the IHO root key is now 2048 bits this requires a fresh re-issue of all certificates anyway. A secretariat working group of participants should be considered, separately from any responsibility with Part 15 (and those relevant parts of Part 17) to act as a forum for ideas and reviews of operating statuses.

Conclusions

There are a number of items to be considered as the edition 5.0.0 data protection scheme is (re-)launched. This paper suggest some which are of the highest priority (as they concern certificates for data producers and distributors).

Recommendations

1. Standardisation of X.509 certificate fields according to the following content (embedding the IHO producer code in the certificate common name). This should be implemented by the IHO as the SA but is not required for standardisation within Part 15 of S-100. It should be considered for the next edition of S-98 to clarify how certificates and authentication are processed by the S-100 ECDIS.
2. The following values are proposed:
    - C (Country) = **ISO Country Code of state making request**
    - ST (State or Province) = **A code reflecting the role of the subject**
    - O (Organisation) = **member state organisation name (text)**
    - CN (Common Name) = **IHO data producer code integer and alpha code (as part of a colon separated MRN), e.g. urn:mrn:iho:aa:1810 or urn:mrn:iho:GB:540.**
3. A commitment to the issuing of signed digital content (catalogues) by the scheme administrator acting on behalf of the IHO and the responsibility of distributors to reproduce them in their entirety. This should be implemented by the IHO Secretariat acting as the Part 15 SA.
4. The launch of the S-100 Data Protection scheme and creation of a single resource to support implementers on the IHO website.

Justification and Impacts

1. The proposals formalises the implementation of the new key length and issuing of new certificates to all participants. It formalises “identity” definition within the IHO and provides a foundation which is machine readable and scalable with no impact on standards or current implementations.
2. The proposal closes potential loopholes and confusion caused by unstructured publicly readable names in certificates issued by the IHO
3. The proposal ensures that all content directly issued by IHO secretariat (acting for IHO members or for the geospatial registry content) is digitally signed and reproduced without change by all scheme participants as S-100 ECDIS is rolled out.

Action Required of S100WG

The S-100WG is asked to:

1. Note the contents of the paper
2. Endorse the implementation by the SA (IHO Secretariat) of Part 15 using
    a. formalised identifiers for participants in the data protection scheme according to the proposed formats
    b. Only signed content in accordance with Part 15 for content distributed by the IHO secreatarita (members and geospatial registry).