[S100TSM9-7.3]

Paper for Consideration by S100TSM9

Tighter control of dataset import to S-100 ECDIS.

Submitted by:	IIC Technologies
Executive Summary:	Exec sum3
Related Documents:	S100WG7-4.3
Related Projects:	S-164, S-100 ECDIS, WEND

Introduction / Background

S-98 Annex C currently contains a number of procedural diagrams and explanations (Appendix C-2) for the import of data to ECDIS. At the moment there are no restrictions on which non-Chart layers can be loaded and portrayed on an S-100 ECDIS.

S-100 Part 15 defines a methodology for digital signing and authentication of all elements of an exchange set. There are a number of developments in the data producer community which have increased interest in how import of S-100 data layers to the ECDIS can be controlled in order to meet the needs of IHO member states. Under S-100 Part 15 and Part 17 a flexible framework can be easily implemented for data management on the ECDIS of all layers (in the same way that S-63 extends S-57 to allow for digital services to be developed)

Each dataset in an S-100 exchange set is digitally signed. Each digital signature authenticates the dataset content against a known identity via a defined producer code. These producer codes are an integral part of the digital signature certificate against which the signature is verified by the ECDIS.

Under the current S-98 ruleset datasets for which the digital signature can not be verified should not be loaded/imported onto the ECDIS (either because the content is corrupt or if the certificate validating the dataset is not itself authenticated by the IHO Scheme administrator).

The consequences of loading invalid or unauthorised data to the ECDIS could be profound and have many well-documented impacts in the cyber security community. The definition of user selected safety contour and water level adjustment annexes in S-98 also have potentially large impacts should users inadvertently load incompatible S-102, S-104 or other data layers to the ECDIS on top of official S-101 charts. Across IHO member states the requirement is different, i.e.

1. Not allowing any overlays on electronic charts other than those which may be mandated (either now or in the future)
2. Allowing overlays from certain specific agencies
3. Allowing only overlays from the same source as that which produces the electronic chart.

Analysis/Discussion

S-100 Part 15 suggests a mechanisms by which this variable requirement can be satisfied, and which provides the correct amount of rigour given the cyber-security and safety risks implicit in overlays to S-100 charts. As stated in the introduction to this paper all datasets must be digitally signed and such signatures carry an immutable tie to an S-100 producer code through the certificate metadata (which contains an MRN of the producer code of the identity being certified).

Digital signatures under Part 15 verify the content of data files (whether dataset, support files or catalogues) against a particular identity contained within a certificate (also delivered with the exchange set). Such certificates must, themselves, validate against the SA certificate which contains the IHO's identity. Each certificate, therefore holds to identities:

1. Issuer (the body who issued the certificate)
2. Subject (the identity which is being authenticate

It is proposed that the following rules should govern the import of all data to the ECDIS, and that these rules are documented in Appendix C-1 of S-98 Annex C (and reflected in S-164 test datasets). It is also proposed that the Appendix C-1 of S-98 is classified as normative (rather than its current status as informative)

Data Import Rules.

S-100 data can only be installed onto an S-100 ECDIS if:

1. Chart data can always be installed as long as at least one valid digital signature exists which is authenticated by a certificate with the data producer MRN as the Subject. These certificates are included in the exchange set and authenticate them against the SA. Note that under S-100 Part 15 there can be other signatures (e.g. from a RENC) but the data producer signature should be authoritative. This restriction could be weakened as an alternative to allow import into the ECDIS if no data producer signature exists if an appropriate warning could be issued to the end user (e.g. if a dataset is only signed e.g. by a RENC)
2. Non-chart data (an "overlay") can only be installed if one or more of the following hold:
    a. It the overlay has the same data producer code as the charts it overlays
    b. It has at least one additional digital signature from the data producer of the charts it overlays (possibly in addition to its own digital signature). So, either the overlay has the same producer code as the chart it overlays or the data producer of the chart has signed the overlay to confirm it is "valid" / "safe".
    c. An extra "authenticating certificate" is included in the exchange set issued by the data producer of the chart authenticating the data producer of the overlay (e.g. issued by the chart data producer MRN code, with a subject of the overlay data producer MRN code). This does not affect the digital signatures of the datasets which are required, the authenticating certificate is included in the exchange set to authorise the overlay producer from the chart producer.

Storage of Certificates

There is currently no requirement to "store" data server certificates on the ECDIS. There is no security risk in doing so, the ECDIS currently stores the SA certificate separately and could easily cache data server certificates without weakening the security of Part 15. This could reduce the number of discrete certificates required for transport of data in, for example, "Update" exchange sets. However, a service provider would then need to ensure the ECDIS has all the certificates it needs and that they are all up to date (with none having expired). In this case the CATALOG.XML validation would have to take into account that certificates could be stored on the ECDIS and not try to validate that every signature entry has a corresponding certificate in every exchange set.

Conclusions

- Strengthening the ECDIS import mechanism makes it less prone to unexpected data import on top of charts which are always required as the fundamental legal minimum.
- Part 15 and its links to the producer code provide a mechanism which is extremely secure and clear. S-98 has much of the necessary procedures already defined and would require a small number of enhancements to define such rules.
- Without such a ruleset the ECDIS is open to import from any IHO authenticated body of any overlay on top of any charts irrespective of conventions, rules or guidance issued by the IHO.

Action Required of S-100WG

The S-100WG is invited to:

Note the paper and discuss proposed changes to S-98 and S-164.