S-100WG7-67.a

Comments on S-100WG7 6.7

(Productionising Part 15 – Identifiers and procedures)

Submitted by:	PRIMAR
Executive Summary:	This paper outlines comments to the proposed productionising of Part 15.
Related Documents:	S-100 5.0.0
Related Projects:	

Introduction / Background

1. At the recent PAC29 meeting the PRIMAR member states agreed to fund a PRIMAR/ECC project focusing on IHO Capacity Building. The specific content of the project is to:

- Update IHO SA (Scheme Administrator) application to support S-100 edition 5.
- Update internal IHB work procedures to reflect standard changes introduced in S-100e5.x.x and the operation of a transition period with both S-63 and S-100e4/e5 protection schemes.
- Provide training of IHB staff in S-100 data protection and SA procedures.
- In-office support to IHB during training session and generation of a new IHO S-100e5 certificate and issuing the first S-100e5 compliant Data Server certificates (to PRIMAR and ECC).
- Establish support routines.

2. IHO director Luigi Sinapi attended the PAC meeting and also suggested that a MoU between PRIMAR and IHO to cover this and relevant activities will be included. Plan is to complete the MoU and the IHO Data Protection capacity building early 2023. All work in this project will be in very close collaboration with IHB staff.

Analysis/Discussion

3. In the introduction the document mentions that S-100WG7 has an action to establish working procedures for the operation of the scheme by the SA. As we were not aware, who is involved and what are their timelines? The same activities are included in the PAC project proposal.

4. Typo on first page where the key length shall be 2048, and not 2948.

5. The same naming principles can also be applied for IHO when they are generating a new S-100e5 X.509 root digital certificate.

6. Document also talks about the encoding of ST (State or province)role of the subject. What are the roles a certificate subject can have within the protection scheme? Data producer, RENC, distributor? Must be clearly defined.

7. It would be nice to establish a common consensus regarding the duration of Data Server certificates. A short duration (one/two tears) will also require that every Data Server sends a new CRS (Certificate Signing Request) at the end of their certificate duration to renew their certificate. Short duration, more workload on IHB. The process is fully automated in the IHO SA application, but it must be run by a human. Currently the Data Server Certificates are issued for 10 years, and IHO root is issued for 50 years.

8. Data Server organisations, S-62 and CN (common name) encoding: Are we sure that all Data Server organisations will have an entrant in the S-62, or is that a pre-requisite to become a Data Server? Both hydrographic offices and any governmental/commercial entities are eligible to become a Data Server.

9. The existing IHO SA application already has functionality to digitally sign files as IHO using S-100e4. Must update functionality to support S-100e5. Suggest any support for S-100e4 is removed at the same time.

10. An OEM system shall have a procedure to authenticate the digital certificates supplied in an exchange set before the enclosed public key can be extracted and used to authenticate the digital signature of a file. There will

not be a need to display the subject identified in a certificate because it does not necessarily say anything about the status of the data they have signed. <it shall provide a warning if the certificate subject can not be authenticated since it is then part of the IHO protection scheme, or an error occurred during the exchange of the dataset. It will for example be possible for a commercial distributor who is also a Data Server to digitally sign data produced by his organisation before it is distributed to their users. The data is still unofficial and can not be used for navigation.

Conclusions
No objections to proposal.

Question is how restrictive IHO will/shall be on this and how much error checking shall be implemented before issuing a data server certificate. The protection scheme will not break or fall apart whatever information is encoded in the proposed fields by the organisation generating a CSR.

Document implies some new user requirements and will require amendment of existing functionality of the SA application.

Action Required of S-100WG5
The S-100WG is invited to:
Note this comment paper.