Paper for Consideration by TSM

PRIMAR input to S-100 Part 15

Submitted by:	PRIMAR
Executive Summary:	After S-100WG finalised S-100 5.2.0, PRIMAR has identified some inconsistencies and the need for some corrections. There is a specific concern regarding the missing explanatory text related to certificate field specific encoding. Whether the proposed amendments can be issued as a clarification edition of S-100 in its current state and approval process should be further discussed by TSM.
Related Documents:	S-100 5.1.0 Part 15 S-98 S-164
Related Projects:	

Introduction / Background

After S-100WG finalisation of S-100 Part15 for S-100 5.2.0, PRIMAR has identified some shortcomings that should be addressed and further discussed. The identified issues discussed in this paper are also available in the comments sheet (Annex A).

The following issues are identified:

1. Add textual information to describe IHO certificate usage as both Scheme Administrator and Data Server.
2. Update openssl sample commands in table 15-8 and 15-9 to reflect ECDSA used with a P-384 curve and SHA-384 algorithm.
3. Add textual information to describe the use of formalised identifiers and roles in the Data Server Certificate, this information must be provided by the applicant in a certificate signing request (CSR).
4. Clarify the encoding of schemeAdministrator in table 8.11.1.

Analysis/Discussion

For details of the issues, refer to Annex A.

Issue 3 will be further discussed in addition to thoughts about implementing the proposed changes in S-100 as clarifications.

Issue 3

As laid out in item 3, S100WG has endorsed the use of formalised identifiers and roles to be included in the Data Server Certificate. S-98 uses the formal identifiers (urn:mrn:iho:org:AAAA:DDDDD) to distinguish between official and unofficial datasets, and this will also be reflected in S-164.

As long as this information is not included in S-100 Part 15, our concern is that this information may end up not being included by the applicant in a certificate signing request (CSR). The question then becomes:
Could we interpret the requirements for formal identifiers and roles in the Data Server Certificate as absolute demands as long as those requirements are not described in S-100 Part 15?

PRIMAR is developing the IHO Scheme Administrator application, and for the application development, the challenge now is whether or not a certificate signing request (CSR) should be discarded if this information is missing.

PRIMAR believes the formal identifiers must be mandatory, and has implemented this as an absolute demand in the IHO Scheme Administrator application.

For the formalised roles for Data Servers we also propose added textual information to clarify that this should also be included in the certificate signing request (CSR).

At the moment this is not implemented as an absolute demand in the IHO Scheme Administrator application, but this can be changed if need be.

S-100 5.2.0 Clarification

We believe that the proposed changes qualify as clarifications to S-100, only highlighting and expanding the information related to already agreed upon elements. They can be considered as non-substantive changes, and as such be introduced without seeking IHO Member States approval (ref S-100 12-2 only demanding member states approval for clarifications and new editions).

Conclusions

- The proposed changes should be included in S-100 Part 15.
    - We seek common agreement for formal identifiers (producer codes) to become a mandatory part of the CSR.
    - We seek common agreement for Data Server roles to become a mandatory part of the CSR.
- A new clarification (S-100 5.2.1) should be issued.

Action Required of TSM

The TSM is invited to:

- Note the paper and discuss the proposed amendments to Part 15.
- Take any action appropriate.

15	PRIMAR	8.5.1		te/ ed	IHO will have both a Scheme Administrator certificate to create scheme Data Server certificates, and an IHO Data Server certificate used to digitally sign and distribute e.g. S-100 portrayal/feature/interoperability catalogues. Important to inform both system developers and users of the protection scheme about these two roles for.	Add the following text paragraph to 8.4.1: *IHO will as scheme administrator issue a scheme root certificate which is available for download on the IHO web site. It will only be used to create Data Server certificates. IHO will also become a Data Server of its own protection scheme and use this certificate kes to digitally sign S-100 standard files; e.g. portrayal/feature/interoperability catalogues.*	
15	PRIMAR	8.4 and 8.4.1	Table 15-8	ed	First bullet point under 8.4 correctly specifies that the ECDSA shall be used with the P-384 curve and SHA-384 algorithm. The openssl sample commands in table 15-8 will not create a SA certificate compliant with this requirement. The new version of the IHO SA application compliant with S-100e5.2 will only create a Data Server certificate if the CSR has been created using the correct algorithms and ECDSA vector.	Change the openssl commands in table 15-8 in accordance with attached example (listed commands are tested and works with OpenSSL v3.1.2)	
15	PRIMAR	8.4 and 8.4.2	Table 15-9	´ed	First bullet point under 8.4 correctly specifies that the ECDSA shall be used with the P-384 curve and SHA-384 algorithm. The openssl sample commands in table 15-9 will not create a Data Server certificate compliant with this requirement.	Change the openssl commands in table 15-9 in accordance with attached example (listed commands are tested and works with OpenSSL v3.1.2)	
15	PRIMAR	8.5.2		te/ ed	The S100WG7 meeting endorsed proposal in S100WG7-6.7 to encode **formalised identifiers** in the Data Server certificates participating in the scheme. This requires that Data Servers must include their Producer Code urn:mrn information when they are generating their Certificate Signing Request (CSR) file to be sent to the IHO SA. This urn information is used by S-98 to distinguish between official and unofficial datasets and it will also be included in the S-164 testdata. Would be appropriate to add a text paragraph informing about the use of urn:mrn.	Add the following text paragraph to 8.4.2: *A Data Server must encode its Producer Code as an urn:mrn entry in the Certificate Signing Request (CSR) file which is sent to the Scheme Administrator. This information will be used by an ECDIS to determine if datasets are official or unofficial. A Data Server can request a Producer Code at the IHO Geospatial Information Registry web site.* *The Producer Code information shall be encoded in the CSR Common Name (CN) field in the following format: urn:mrn:iho:org:AAAA:DDDDD.*	
15	PRIMAR	8.4.2		te/ ed	The S100WG7 meeting endorsed proposal defined in S100WG7-6.7 to encode the **role** of a Data Server participating in the scheme. This will require that the	Add the following text paragraph to 8.4.2:	

					Data Servers must encode their role information when they are generating their Certificate Signing Request (CSR) file to be sent to the IHO Scheme Administrator. The role information is used by S-98 to distinguish between official and unofficial datasets and it will also be included in the S-164 testdata. Would be appropriate to add a text paragraph informing about the use of roles, and meaning of values.	*A Data Server must encode its role in the Certificate Signing Request (CSR) file which is sent to the Scheme Administrator. Role is encoded in the certificate State or Province field (ST) in the CSR file in accordance with one of the following options:* ● ***DATA_PRODUCER*** *- producing data content for live navigation under SOLAS. This data is "official"* ● ***OTHER_DATA_PRODUCER*** *- produce data content which is "unofficial"* ● ***DATA_AGGREGATOR*** *- RENCs/Aggregators - validate, distribute and (sometimes) digitally sign data on behalf of their members. These organisations do not create data content but can "stamp" data as "official"* ● ***AGGREGATOR*** *- aggregate data together for the purposes of running a service for end users. They can only digitally sign datasets.* ● ***SCHEME_ADMINISTRATOR*** *– IHO as Scheme Administrator (only for use by IHO)*	
15	PRIMAR		Table 8.11.1	ed	PRIMAR has seen many examples of different encodings of schemeAdministrator; for example root, IHO, urn:mrn etc. Add correct encoding in table 8.11.1 to remove any ambiguity. Other attributes include example encoding, e.g. productIdentifier, optimumDisplayScale, identifier	Add the following text to the schemeAdministrator Remarks column: *The encoding of IHO as schemeAdministrator is <S100SE:schemeAdministrator id="IHO"/>*	

New table 15-8 commands:

Task	**Command**

SA-1: Create the Scheme Administrator private key using ECDSA algorithm with vector P-384	`openssl ecparam -name secp384r1 -genkey -out sa-privatekey.pem`
SA-2: Create Scheme Administrator self-signed root key	`openssl req -new -x509 -key sa-privatekey.pem -sha384 -out sa-root.crt -days 365`
SA-3: Create and sign a Data Server certificate	`openssl x509 -req -in ds.csr -CA sa-root.crt -CAkey sa-privatekey.pem -out dataserver.crt -sha384 -days 365`

New table 15-9 commands:

Task	**Command**
DS-1: Create the Data Server private key using ECDSA algorithm with vector P-384	`openssl ecparam -name secp384r1 -genkey -out ds-privatekey.pem`
DS-2: Save Data Server public key associated with private key	`openssl pkey -in ds-privatekey.pem -pubout -out ds-publickey.pem`
DS-3: Create Data Server certificate signing request to be sent to IHO SA. Note requirements for encoding certificate Common Name (CN) and State or Province (ST)	`openssl req -new -sha384 -out ds.csr -key ds-privatekey.pem`
DS-4: Verify signed Data Server certificate received from SA	`openssl verify -verbose -CAfile sa-root.crt dataserver.crt`

DS-5: Create a signature for the file hw.txt	`openssl dgst -sha384 -sign ds-privatekey.pem -out signature.bin hw.txt`
DS-6: Encode the signature from DS-5 as Base64	`openssl enc -base64 -in signature.bin -out signature.b64`
DS-7: Extract the Data Server public key from the Data Server certificate	`openssl x509 -in dataserver.crt -pubkey -noout -out ds-publickey.pem`
DS-8: Encode the signature in digital form	`openssl enc -d -base64 -in signature.b64 -out signature.bin`
DS-9: Verify the signature of the file hw.txt	`openssl dgst -sha384 -verify ds-publickey.pem -signature signature.bin hw.txt`