comments and editorial observations

Date: 21.08.2023	Document: **S100 Ed. 5.1.0 Part 15**

1	2	(3)	4	5	(6)	(7)	
Component	**CO[1]**	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the CO[3]**	**Proposed change by the CO**	**Secretariat observations** on each comment submitted
	DE	Part 15	In general	ge	Due to the length of the commentary, it is included as an annex to this document. See also Annex Scenario A & B	Establish a complete certification chain through a global certification authority.	
	DE	Part 15	In general	te	The description of the certificate revocation process is missing. How is this handled if the systems do not have an internet connection? See Annex Scenario C	Describe the process of revoking certificates.	
	DE	Part 15	In general	te	There is no description of the general validity of the root certificate. In our view, this is essential to plan for the potential impact on client system update cycles.	Define the general validity timeframe of the root certificate, e.g. 10 years.	
	DE	15-6.2.1	1. paragraph	te	Why is the highest level of encryption allowed by the AES standard not used? The reason for the weaker encryption is not apparent. Furthermore, the weaker encryption does not correspond to the current state-of-the-art.	Use of AES-256 or disclosure of the reason for the weaker encryption.	
	DE	15-8.4	1. paragraph No. 1.	te	Why are the keys only 2048bit long and not 4096bit? Shorter keys weaken the security of the system. Furthermore, this does not correspond to the current state-of-the-art. According to the national guideline (BSI TR-02102-1), the key length should be at least 3000bit from the year 2023.	Use of 4096bit keys or disclosure of the reason for the 2048bit keys.	
	DE	15-8.4	4. paragraph	ge	Since the S-100 Ed. 5.0.0 is released, the root certificate should also be available on the website. Unfortunately, we could not find it.	Publish the root certificate or a better description of the access.	

1 **CO** = Contributing Organisation (HOs should use 2 character codes e.g. FR AU etc.)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

3 Whilst not compulsory, comments are more likely to be accepted if accompanied by a proposed change.

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)	
Component	**CO[1]**	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment[2]**	**Comment (justification for change) by the CO[3]**	**Proposed change by the CO**	**Secretariat observations** on each comment submitted
	DE	15-8.4	5. paragraph	te	Why is SHA256 used instead of SHA3-384? The longer the hash value, the more unique it is. SHA3-384 is also not more costly or slower to generate than SHA256.	Use of SHA3-384 or disclosure of the reason for the SHA256.	
	DE	15-8.4	5. paragraph	te	Why is the key length for file-based authentication now only 1024bit? According to the national guideline (BSI TR-02102-1), the key length should be at least 3000bit from the year 2023.	Use of 4096bit keys or disclosure of the reason for the 2048bit keys.	
	DE	15-8.10	1. paragraph	ed	“In order to support discoverability of Part XX Exchange Set resources the following MRN namespaces are defined by this Part of S-100.”	Part XX, should be replaced with the correct part number.	

1 **CO** = Contributing Organisation (HOs should use 2 character codes e.g. FR AU etc.)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
3 Whilst not compulsory, comments are more likely to be accepted if accompanied by a proposed change.
NOTE Columns 1, 2, 4, 5 are compulsory.

Annex

Comment

In the BSH's opinion, it is imperative to guarantee comprehensive protection of maritime data in light of the escalating threat scenario in the domain of cybercrime and political instability. Part 15 of S-100 Ed. 5.1.0 already describes some steps for this, but from the BSH's point of view, these are not sufficient. For example, the national guideline "BSI TR-02102-1" obligates German authorities to use stronger encryption techniques from the year 2023 than those provided for in the S-100. Particular attention is given to key lengths of at least 3000 bits. This also includes an IHO root certificate that has been issued by a global certification authority. From the perspective of the BSH, a self-signed root certificate issued by the IHO is not sufficient to safeguard security-relevant data, such as S-102, S-131, etc. The publication process described in Part 15 chapter 8.4 paragraph 4 presents a potential risk of a self-signed certificate. The publication of the root certificate for download on the website of the IHO presents an opportunity for attackers to compromise the initial certificate chain. A cyberattack on the IHO's website and the replacement of the root certificate could have a dramatic impact on subsequent processes. An attack such as this increases the risk of manipulated datasets within the S-100 security environment.

More detailed information on German security regulations can be found in the various guidelines published here (all in English):
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

Scenario A – Signing nautical publications in PDF

Chapter 15-8.1 paragraph 5 of S-100 Ed. 5.1.0 Part 15 outlines that the HO certificate can be utilized to sign any files. Therefore, the BSH could use the certificate to sign NTMs, for example.
It is possible to use NTMs outside of the S-100 Protection Scheme, for example on smartphones, tablets, or private PCs. On these devices, the IHO root certificate is usually not installed, but the certificates of the global certification authorities (CA) are.
NTMs can be downloaded from the BSH website free of charge. When the customer does so, their PDF reader will indicate that the certificate cannot be verified. If deemed necessary, the customer shall approach the BSH and lodge a complaint regarding inaccurate data. The BSH must inform the customer that the issue is solely attributed to the absence of the root certificate from the IHO and that it must be installed manually.
The customer is unhappy with the extra effort and likely does not know how this is done. BSH must explain to the customer what needs to be done, and for every possible device. After all, we simply want satisfied customers. It is also evident that the BSH will be overburdened with tasks that are beyond its scope. Finally, everyone is unhappy, the customers and the BSH.

Scenario B – Office (production) software

The BSH receives signed / encrypted test data. The IHO root certificate is required for verification or viewing. However, this is not installed by default on the BSH PCs, virtual computers and servers because they are not part of the S-100 Protection Scheme. The BSH central IT will refuse to install a self-signed certificate in a protected government environment.
Will the production software (Caris, 7Cs, ESRI, Dkart) automatically install the root certificate as well or is this a task for the HO's?

Scenario C – Revoke process

The initial situation is that several national authorities produce S-100 products. All authorities are in possession of a corresponding IHO certificate. Due to political considerations, it has been determined over time that in the future, only a singular national authority shall be responsible for the production of S-100 products.
How will the certificates of the authorities that no longer produce S-100 products be withdrawn to prevent misuse?

How are the ECDIS systems aware that new records produced after a certain date are invalid with the withdrawn certificate?