Paper for Consideration by the HSSC-12

IEC Activities affecting HSSC

Submitted by:	Hannu Peiponen / IEC TC80 Chair
Executive Summary:	This paper explains status of IHO related issues within IEC Technical Committee 80 (TC80).
Related Documents:	HSSC11-07.4A_IEC_Activities_affecting_HSSC_2019
Related Projects:	N/A

Introduction of S-101 or S-100 into IEC 61174 ECDIS standard

Introduction / Background / Analysis / Discussion

1. In the IEC TC80/Plenary October 2019 meeting IHO informed IEC TC80 about the IHO plan to introduce S-101 ENC charts as alternative for S-57 ENC charts for mandatory implementation by ECDIS with in-force date set as 1st Jan 2024. The IEC TC80/Plenary meeting discussed on the topic and felt that the issue was not mature enough in 2019 for decision making and set a task to secretariat of IEC TC80 ask again opinion of the National Committees of IEC TC80 in year 2020.

2. The plan of the secretariat of IEC TC80 was to ask opinion of the National Committees after IMO has made a decision how to proceed with the IHO initiative to introduce the dual fuel S-57 & S-101 ECDIS. It was assumed that IHO will raise the issue in IMO NCSR-7 January 2020 and that IMO MSC-102 May 2020 would make decisions based on IHO initiative. However, the Covid-19 pandemic cancelled the May 2020 meeting of IMO MSC-102 and there is not yet any clear vision if the time schedule proposed by IHO to IMO will be the IMO decision or if the time schedule will be amended. As result IEC TC80 has not yet asked opinion of the National Committees.

3. For your information the normal timetable for the development of a new edition of an IEC standard is 2 years of committee work to draft the Committee Draft for Vote (CDV) plus 1 year of voting & comment process to complete the draft as International Standard. It should be noted that all technical details referenced by the draft for an IEC standard should be completed before the IEC workgroup completes the CDV. This means that S-101 related IHO standards including both the specification and testing part should be published as final versions before the assumed completion of the CDV. Another point to note is that on the day of publishing a New work item Proposal (NP) or Questionnaire (Q) for vote by the National Committees of the IEC TC80, the proposed topic should be mature enough for the National Committees to understand that now it is the time to create the new edition of the IEC 61174 ECDIS.

4. The role of IEC TC80 is to provide standards to be available for the user community. IEC TC80 itself has no opinion on how much time the user community needs to be ready to use a newly published IEC standard.

Action Required of HSSC

5. The HSSC is invited to:

1. Note that IEC follows the progress about introduction of S-101 or S-100 into IMO requirements for ECDIS

Data cyber security requirements for navigation equipment (IEC 63154)

Introduction / Background / Analysis / Discussion

6. The IEC standard requesting authentication of all external data files at import into a navigation equipment is IEC 63154. The work on this standard begun in 2017. The work has reached CDV (Committee Draft for Vote) stage and the CDV was approved by voting in September 2020. The next step is creation of FDIS (Final Draft International Standard), voting on the FDIS and the publication as International Standard is forecasted for August 2021.

7. IEC raised this issue of cyber security for the first time at HSSC-10, May 2018. The background information and analysis are still the same as the years before. Also, the conclusion of IEC – the authentication of data from IHO sources should be overarching i.e. including all auxiliary files. See HSSC10-07.4A_IEC_Activities_affecting_HSSC_2018.

8. IEC has noted progress by IHO

- For S-57 ENC charts IEC has noted that work is still going on by IHO ENCWG. The issue has been discussed at ENCWG meetings 2018 and 2019. Meetings have set tasks to both draft solution for the issue (i.e. new edition of S-63) and to seek approval of industry for the solution. IEC understands that international organizations need time to develop and agree standards. Therefore, currently IEC is pleased to follow up the progress by IHO ENCWG.

Action Required of HSSC

9. The HSSC is invited to:

1. Note that IEC follows the progress about the solution (new edition of S-63) for S-57 ENC charts

S-421: Route Plan based on S-100 (IEC 63173-1)

Introduction / Background / Analysis / Discussion

10. IEC TC80 has established WG17 to address CMDS (Common Maritime Data Structure). The workgroup was created in October 2015. Convenor is Dr. Kwangil Lee (KMOU, Korea). Within IEC TC80 all CMDS works related with shipborne system will be handled in this workgroup. IEC TC80 applied and was granted S-100 domain ownership in December 2016.

11. Under progress is **S-421 Route Plan Exchange** (also known as **IEC 63173-1**). The base is already published Route Exchange, IEC 61174 Ed4 ECDIS, Annex S, extended by ideas from Testbeds, especially STM validation and SMART navigation. Timeline is:

- The related IEC workgroup has completed drafting of the CDV in September 2020
- IEC approval process consisting of CDV and FDIS comments & voting will use the remaining of year 2020 plus year 2021 and the publication of IEC 63173-1 is assumed around 2nd half of 2021

12. The object model of the **S-421 Route Plan Exchange** reflects the needs of the use cases:

1. Route cross check: Ship sends route for check by shore, for example by VTS
2. Flow management: Shore, for example VTS, organize the schedules of ships for fluent sailing
3. Enhanced monitoring: Shore monitor sailing of the ship against the route plan
4. Ice navigation: Traffic management for ice covered areas provides routes for ships
5. Under keel clearance management: This operates together with S-129
6. Fleet route planning: A tool for shipowner to manage fleet
7. Chart management: Chart seller provide charts based on the route plan
8. Route optimization: Ship uses 3rd party service to optimize route plan
9. Port call synchronization: Ship participate in port call optimization or just in time arrival scheme
10. Reference route: Shore provide reference route to sail for example from a pilot point to port
11. Search and rescue: MRCC instruct ships about SAR sailing patterns

Action Required of HSSC

13. The HSSC is invited to:

1. Note the information provided

Secure exchange and communication of S-100 based products (SECOM) (IEC 63173-2)

Introduction / Background

14. The background of the SECOM is the e-Navigation testbed "STM validation project" which tested e-Navigation related file transfers using SOA (Service Oriented Architecture) principles with about 400 real ships and multiple VTS/Ports.

15. The IEC 63173-2 standard is intended to be a gap-filler to provide standardized communication infrastructure between shore and ships for bi-directional transfer of files related to the e-Navigation. It is assumed that majority of such files may be based on IHO S-100 although the SECOM infrastructure is in principle capable to transfer any anonymous file. Excluded from SECOM is services which need data streaming and which cannot be converted as a series of separate data files.

16. Latest version available is a Committee Draft (CD), IEC TC80/956/CD. The Committee Draft for Vote (CDV) is planned for October 2021.

17. The planned publication as international standard is 2nd half of 2022.

Technical description

Cyber security and high-level approach

18. A common set of key words in cyber security is authentication, integrity check and confidentiality. SECOM facilitate all of them. For the data protection i.e. protection of payload of the data transfer SECOM provides end-to-end digital signatures (facilitate both authentication and integrity check) and optionally encryption (facilitate confidentiality). The protection of confidentiality is optional as the nature of many maritime e-Navigation services is public broadcast. For the communication protection (i.e. protection of commands within SECOM service API) SECOM provides channel protection.

19. The ship side of the SECOM is based on commercial vendors providing the "last mile" or the "hop" i.e. communication from shore to ship. The commercial vendors will provide a service running off-ship (for example on shore or in cloud) which represent each individual ship towards SECOM. Within the solution of the commercial vendor it is assumed that the solution is based on the ship pulling data from the service of the commercial vendor (i.e. a ship is not exposed for easy hacking through the push method). This architecture allows both pull and push (i.e. subscription) methods between the shore actors and the service of the commercial vendor (see green area in figure 1). Onboard there is a standardized 460-Gateway (IEC 61162-460). This gateway is assumed to provide a file storage called DMZ. Onboard navigation equipment will store and fetch the data payload files from this DMZ (typically seen as mapped network drive in the local area network (LAN) of the navigation). It is assumed that navigation equipment sees the same structure as specified by individual data product standards (for example same folders and files as described in IHO S-63 for the distribution of IHO S-57 ENC charts).

20. SECOM use the IHO S-100 Baseline Ed 4.0.0 Part 15 for end-to-end authentication based on digital signatures (IHO Data Protection). For this method the gap has been key distribution. The easy case is the "broadcast style" data (i.e. ENC charts, nautical publications, weather forecast, etc.) from shore authorities to vessels as this could be based as IHO being scheme administrator and holder of the root key (i.e. as today for IHO S-63 for S-57 ENC charts). The not yet specified case, i.e. the gap, for key distribution has been between ships and shore actors such as VTS, Port operator, Weather optimization service, etc.

21. SECOM solution is to use a PKI (Public Key Infrastructure) where the planned Maritime Connectivity Platform (MCP), an initiative of IALA, facilitates infrastructure of e-Navigation (i.e. Identity Registry). For key distribution purposes two services in the Identity Registry are needed: 1) possibility to download "public key" of any identity in the Identity Register (this public key would then be used to authenticate and to integrity check received files); and 2) possibility to register the "public key" for an identity in the Identity Register using a cyber secure method (draft idea is based for a one time token obtained from MCP which is a part of the cyber security arrangement to register the public key).

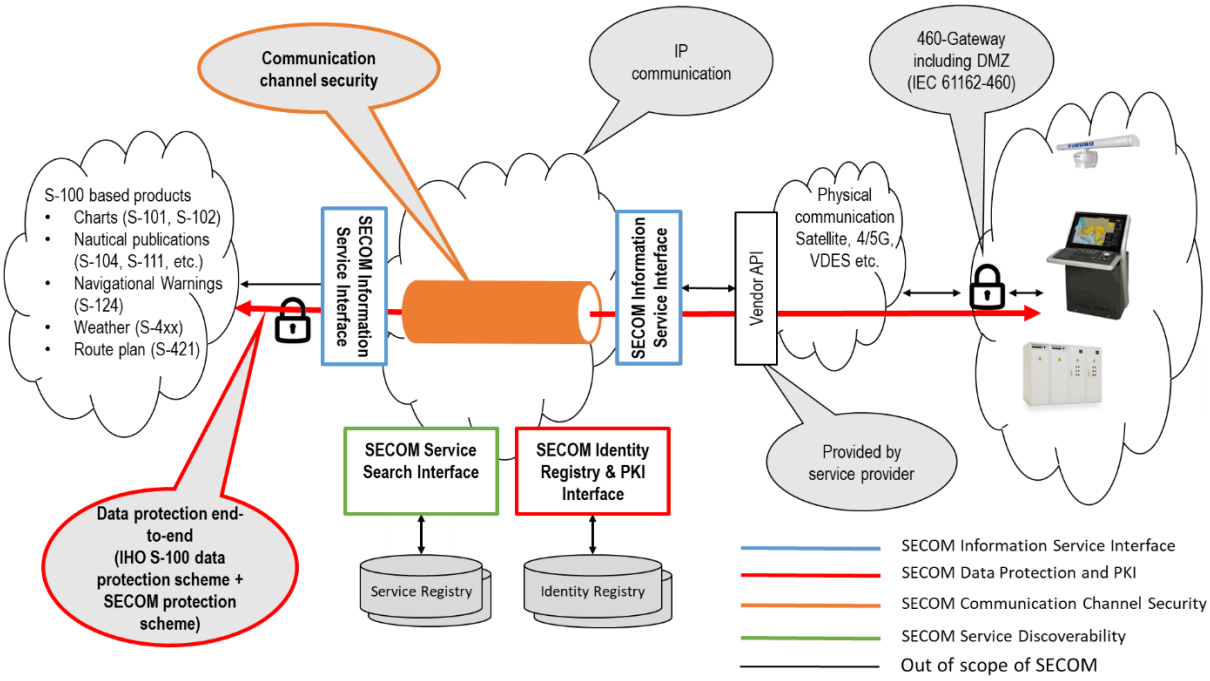

Figure 1: High level description of IEC 63173-2

End-to-end data protection and channel protection

22. SECOM applies defence in depth or onion principle (i.e. several layers) for cyber security. SECOM uses both of these two different approaches (end-to-end data protection and channel protection) to the cyber security, see figures 1 and 2. Application layer uses the end-to-end principle (i.e. origin provides digital signature as per IHO S-100 Part 15 and final end user authenticates it). Transport layer uses channel protection (TLS)

23. End-to-end protection, for example IHO S-63, IHO S-100 Part 15, etc., is based on the idea that the transfer of the data may go through uncountable and uncontrolled hops from source to the final consumer. The cyber security is provided by a digital signature related to the data. This digital signature is then used by the final consumer to authenticate the source and to check the integrity of the content of the data.

24. Channel protection, for example TLS, VPN, etc., is based on idea that there is a secure tunnel between the parties and that therefore data within the secure tunnel is protected even when the there is no authentication nor encryption of the data itself.

25. It is well known that the complete transfer route of data between ships and shore very often go through proxy-servers (for example used by the ICT-department of the ship owner to control the data flow between shore and vessel) which will either block or do not facilitate TLS, VPN, etc. Therefore, the main mitigation against cyber threats is based on end-to-end protection. The addition of channel protection has merits in limiting the number of attempts to attack by limiting number of cases where hackers are able to knock the door. Therefore, the channel protection is used to further improve the cyber security.

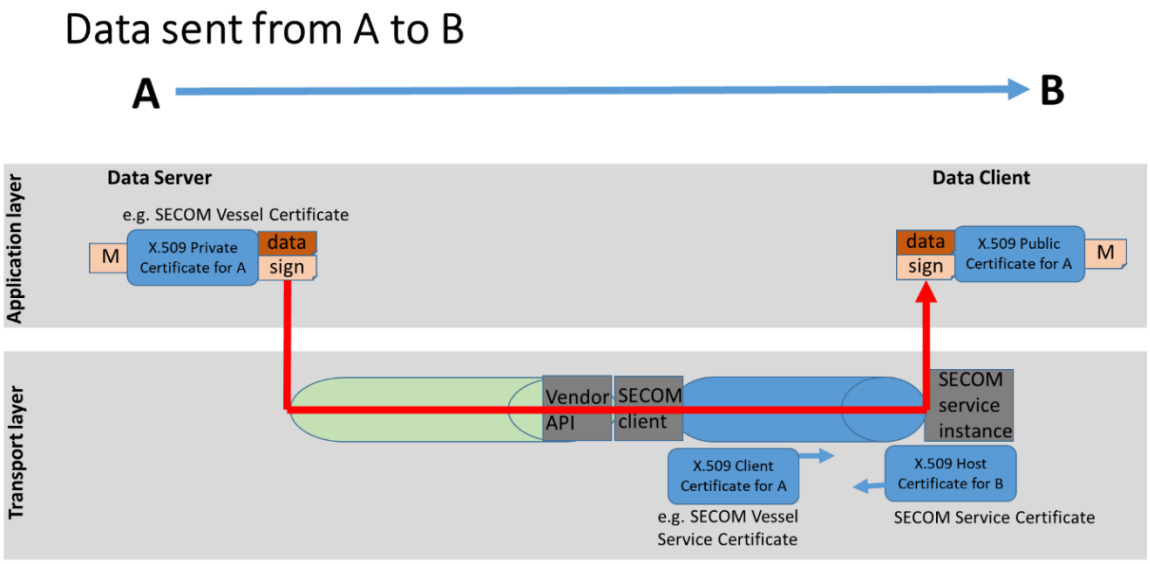

Figure 2: Overview of signature/certificate usage

Key management for application layer "end-to-end data protection" (SECOM PKI)

26. IHO S-63 and IHO S-100 Part 15 facilitate Public key Infrastructure (PKI) key management for data files originating from Hydrographic Offices to ships. For these use cases IHO acts as scheme administrator. Other use cases, for example route plan exchange between ship and VTS centre, may not be able to join to the IHO administrated scheme. SECOM PKI is an alternative method to facilitate private/public key management when the sender of data cannot join IHO administrated scheme. The PKI is used to facilitate authentication and integrity check of the data payload.

27. The method is SECOM PKI (public key infrastructure). The principle is that the origin keeps always its "private key" as a local secrecy. The origin submits its "public key" through SECOM service API to the "Identity Registry". The receiver of the data fetches the "public key" of the origin from the "Identity Registry" through SECOM service API. The "Identity Registry" is a component that could be provided by several providers. Currently the STM project influenced industry consortium (Navelink) and the Korean government are setting up operational instances of Maritime Connectivity Platform (MCP) to facilitate availability of "Identity Registry" for use by PKI infrastructures.

28. Figure 3 shows an example of how the above principle is used for data transfer from ship to shore.

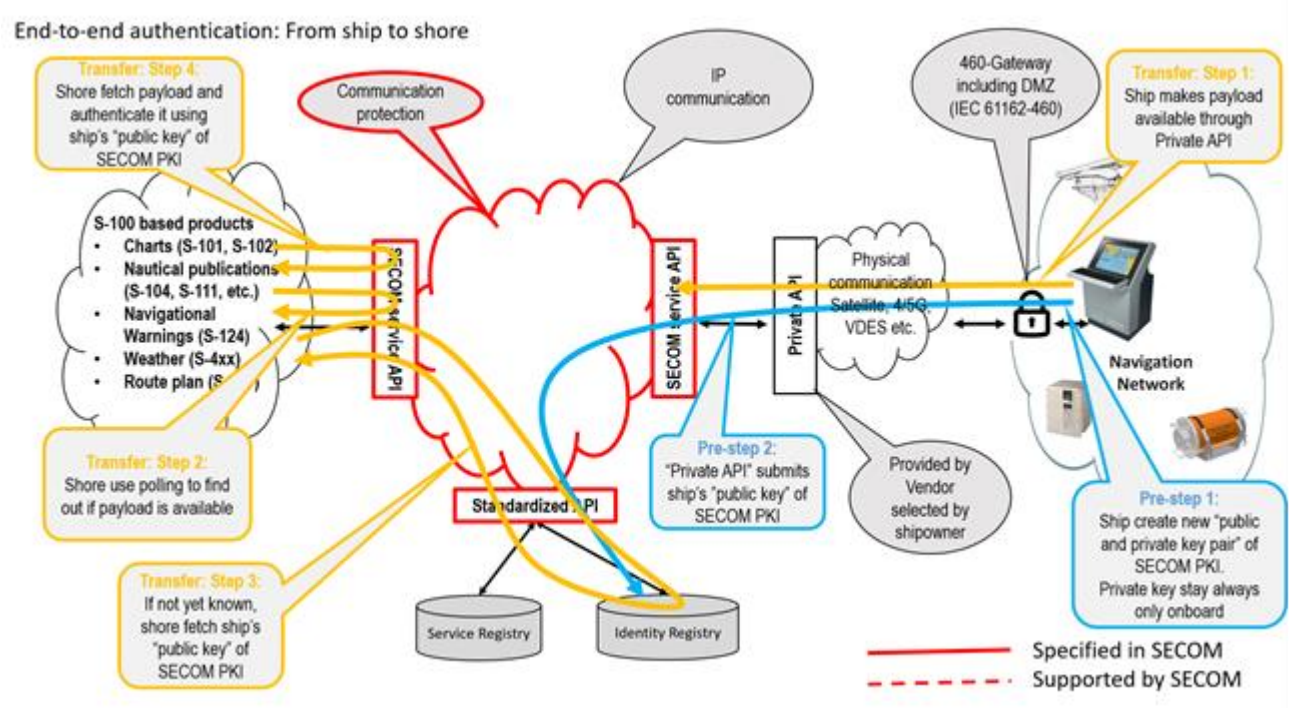

Figure 3: Application layer key management and data transfer

Key management for transport layer "channel protection"

29. This method uses TLS (Transport Layer Security): HTTP/1.1 according to RFC-7231; HTTP over TLS according to RFC-2818; TLS version 1.1 (RFC-4346), TLS version 1.2 (RFC-5246) or TLS version 1.3 (RFC-8446); Mutual authentication, where both client and server authenticate each other using certificate-based TLS mutual authentication (TLS client-side X.509 authentication), see figure 4.

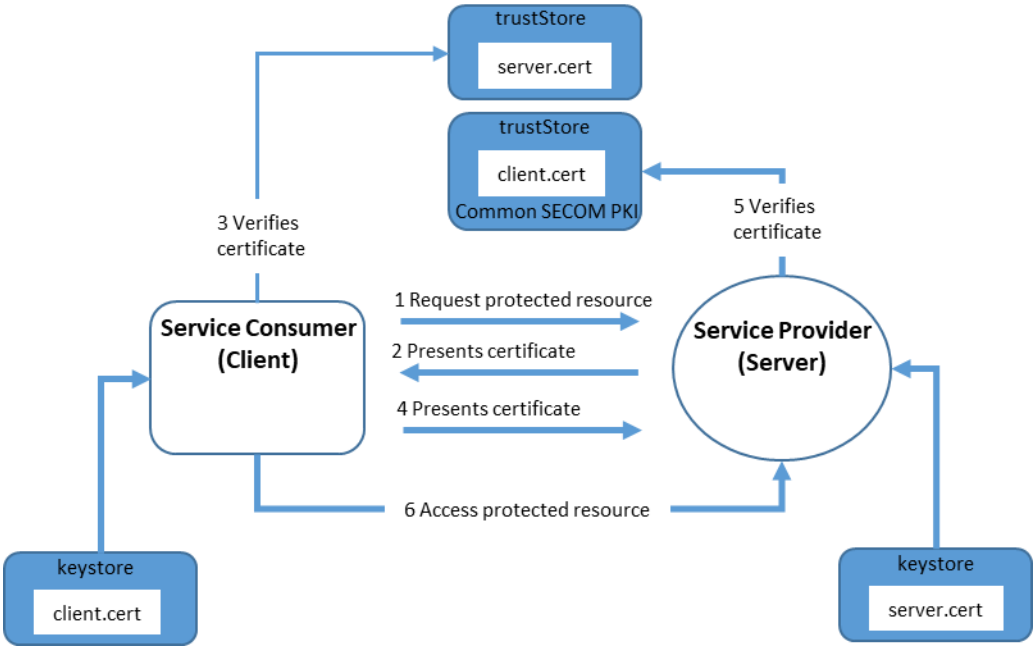

Figure 4: Principle of transport layer mutual authentication

Optional "data encryption" - confidentiality

30. Many data transfers over SECOM do not need protection of confidentiality (i.e. that only sender and receiver knows the content). The other use case for data encryption is commercial revenue collection (i.e. permits to use the data are sold by a commercial entity). SECOM is neutral on the issue of commercial revenue collection – the data payload can be encrypted by proprietary methods and the payload could include separate parts which contain the permits (an example of such a revenue collection method is IHO S-63 used for commercial sale of IHO S-57 ENC charts). Some examples of data which do not need encryption by SECOM: S-124 Navigational Warnings, etc. Some use cases, for example S-421 route transfer for weather routing, may need encryption. SECOM standard includes a standardized method for this kind of purposes.

31. SECOM use the S-100 Part 15-6 specified encryption algorithm Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode of operation. AES is symmetric algorithm and the encryption key used by AES is called "secret key". The "secret key" is used both to encrypt and decrypt the data payload.

32. The sharing of "secret" keys could be based on IHO published method (for example S-63 or S-100 Part 15-7). In many use cases and especially when source of data is a ship the IHO published method of sharing of the "secret" key cannot be used. For such use cases SECOM specifies how the "secret key" can be securely transferred from the origin to the receiver: The principle is similar to the Diffie-Hellman key exchange and is based on use of asymmetric algorithms to protect the "secret key". The origin encrypts the "secret key" using the "public key" of the receiver from the SECOM PKI (i.e. "public key" used by application layer). Then the encrypted "secret key" is signed using the "private key" for SECOM PKI of the sender. Both the encrypted "secret key" and the digital signature is then transferred to the receiver. The receiver first authenticates the digital signature using the "public key" of the origin from the SECOM PKI. If the authentication pass, the receiver decrypts the encrypted "secret key" using receivers "private key" for SECOM PKI.

Action Required of HSSC

33. The HSSC is invited to:

1. Note the information provided