Information for the S-100WG-5

IEC report of IHO S-100 related items

Submitted by:	Hannu Peiponen / IEC TC80 Chair
Executive Summary:	This paper is about ongoing processes by IEC TC80 related to IHO S-100 concept
Related Documents:	N/A
Related Projects:	N/A

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

Introduction / Background / Analysis / Discussion

1. The planned target of publishing is Apr 2021, but the process is behind the schedule. The publishing could move to 2020.

2. Current work is focused on the use cases. More government organizations have joined the related IEC workgroup with their specific use cases. The object model of the Route Plan reflects the needs of the use cases. Current list of uses 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 provide 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

3. Latest version available is a Committee Draft (CD), IEC TC80/948/CD

4. Next meeting of the related IEC workgroup (IEC TC80/WG17) is 25th – 27th Feb 2020 (i.e. the week before IHO S-100WG-5 meeting).

Action Required of S-100WG

The S-100WG is invited to:

1. Note the information provided

Secure Communication (SECOM) (IEC 63173-2)

Introduction / Background

1. 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.

2. This standard is intended to be a gap-filler to provide standardized communication infrastructure between shore and ships for 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.

3. Latest version available is a Committee Draft (CD), IEC TC80/956/CD

4. The planned publication as international standard is summer of 2022.

Technical description

Cyber security and high-level approach

5. 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.

6. The vessel 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).

7. 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.

8. 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. For key distribution purposes two services in the Identity Register 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).

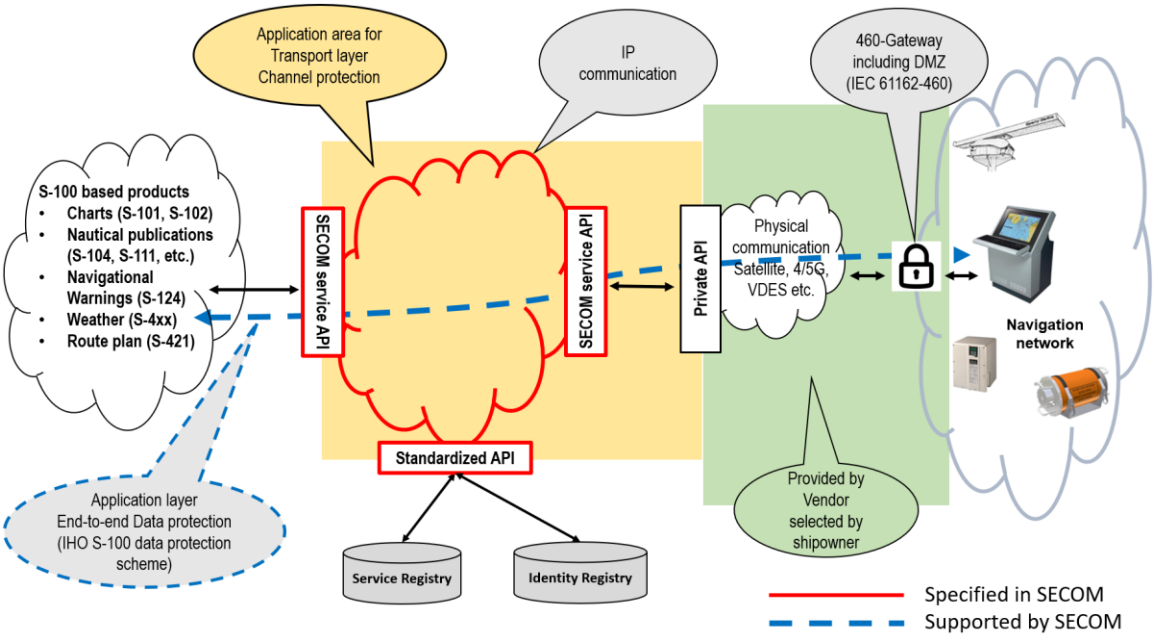

Figure 1: High level description of IEC 63173-2

End-to-end data protection and channel protection

9. 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 provide digital signature as per IHO S-100 Part 15 and final end user authenticate it). Transport layer uses channel protection (TLS)

10. 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.

11. End-to-end protection, for example IHO S-63, IHO S-100 Part 15, etc. is based on 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.

12. 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.

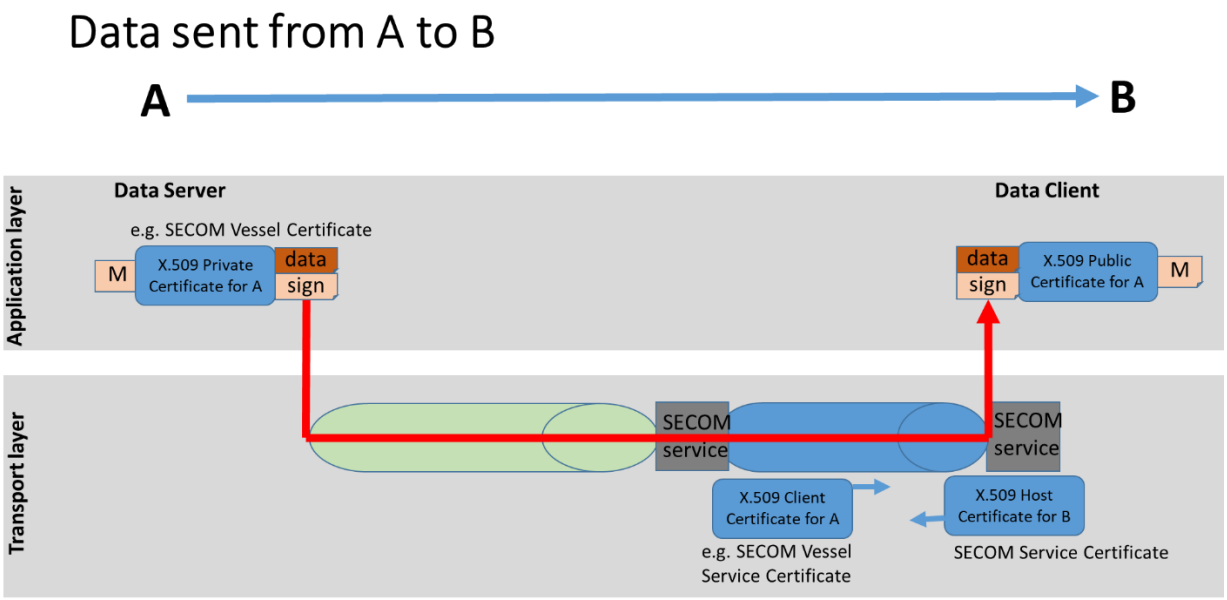

Figure 2: Overview of signature/certificate usage

Key management for application layer "end-to-end data protection" (SECOM PKI)
13. This is to facilitate authentication and integrity check of the data payload.

14. 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 register". The receiver of the data fetches the "public key" of the origin from the "Identity register" through SECOM service API. The "Identity registry" is a component that could be provided by several different providers. Currently the STM industry consortium and the Korean government are setting up operational instances of PKI infrastructures.

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

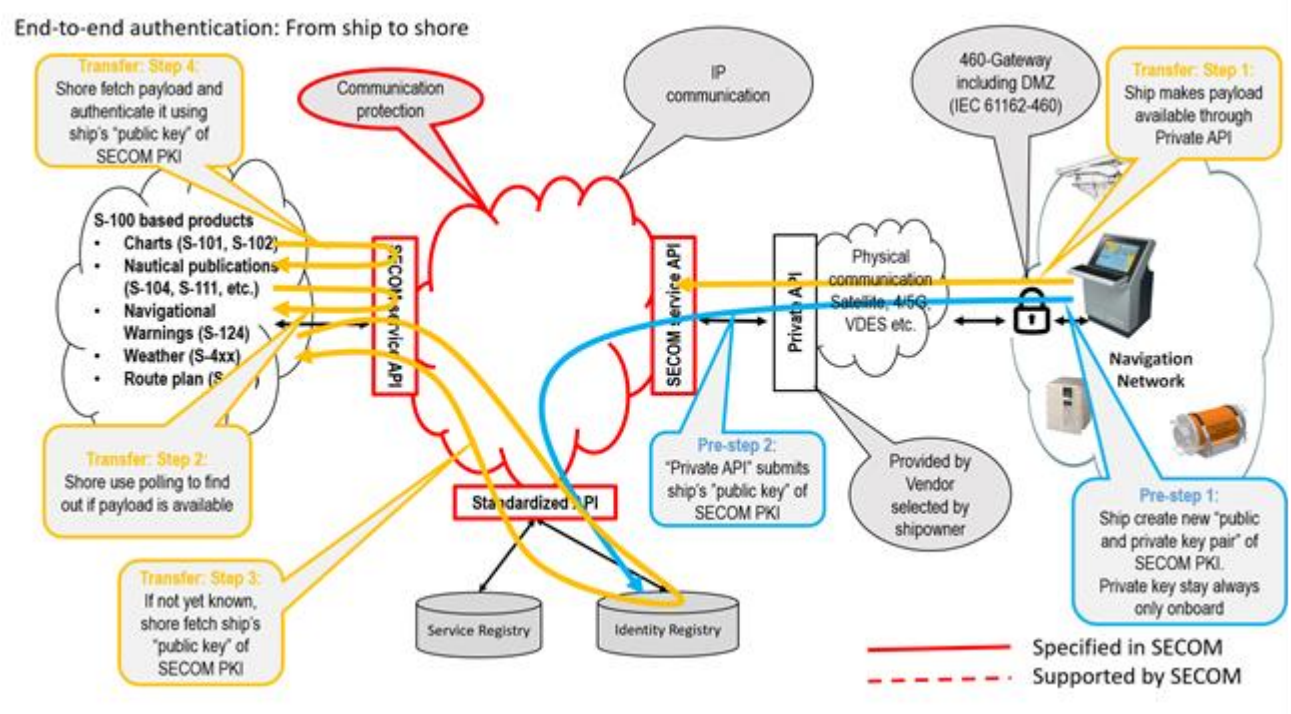

Figure 3: Application layer key management and data transfer

Key management for transport layer "channel protection"
16. 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.

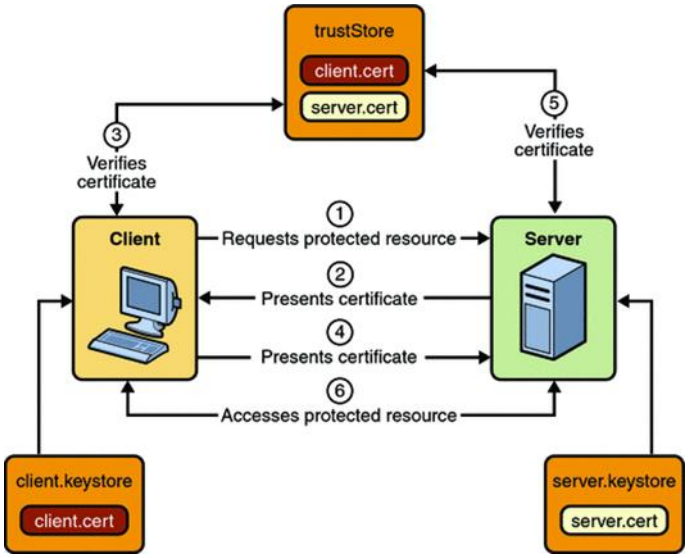

Figure 4: Principle of transport layer mutual authentication

Optional "data encryption" - confidentiality

17. 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.

18. SECOM specified encryption algorithm is 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.

19. SECOM specify 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 S-100WG

The S-100WG is invited to:

1. Note the information provided