NAVELINK

Developer forum

30-11-2023

Navelink.org

Agenda

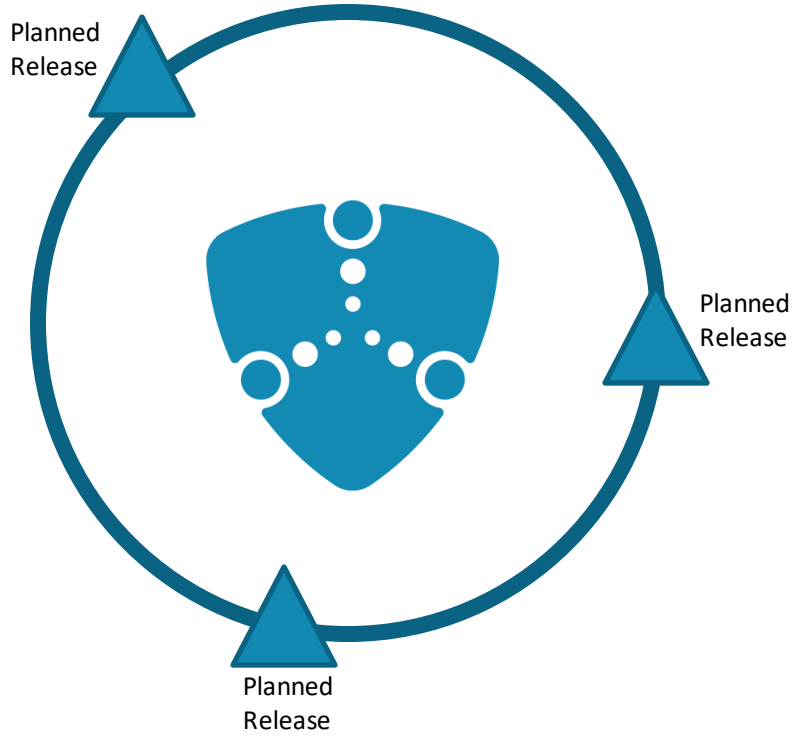
1) Navelink Platform status & update
2) Navelink Roadmap (Head of concept Navelink)
3) Service development discussions & information
   a) Forum service developers (Each developer)
   b) Forum security and interoperability (Each developer)
   c) Ongoing work within the STM-community (Trello) (Each developer)
4) Overview of Navelink usage
5) Q&A
   a) New questions (All)
6) Demo – How to Implement SECOM Upload interface by Mikael Olofsson (Navelink)
7) Discussion: Navelink + REST + MMS + VDES
8) Closing remarks

1) Navelink Platform status & update

- Since the last meeting:
  - Work in progress with creation of SECOM Hotel
- Future
  - Continued work with the creation of SECOM Hotel
    - Preliminary Q1

Received questions

-



2) Navelink Roadmap

1-2 years

2-5 years

Support new Service Specifications and Designs

Increase VDES support

Add GetPublicKey

Add MMS support

Increase SECOM Compliance

Add SECOM Hotel

Add SecretKeyExchange

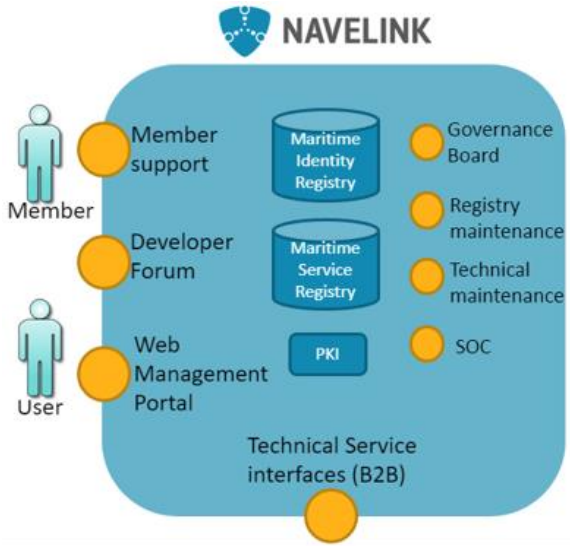
Add MRR usage

Add Service Ledger support

Enable subscription on Navelink technical notes

Enhance functionality to host payload formats

Add support for Service Payment

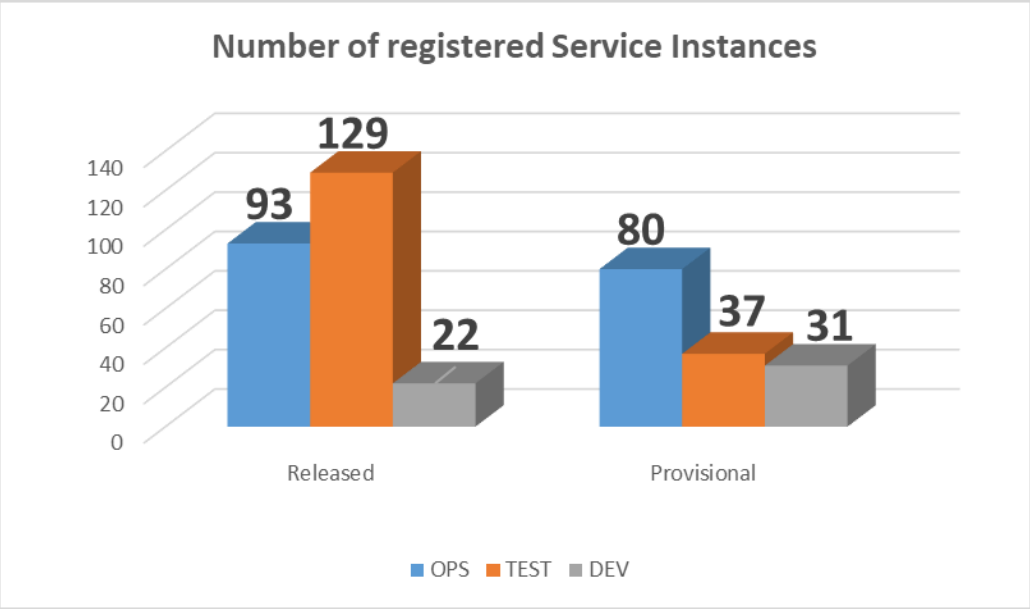


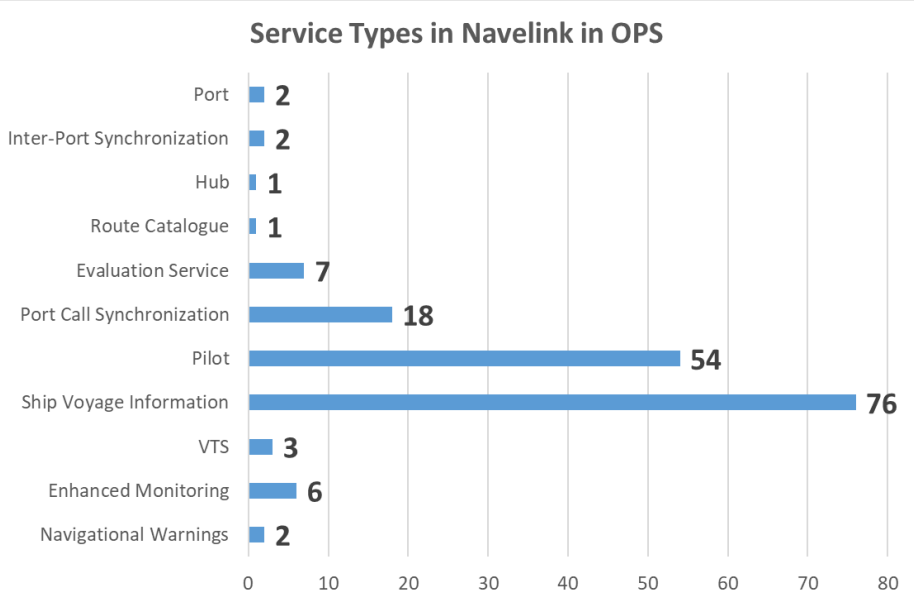
3) Service development discussions & information

- Forum service developers
  - Common discussions
- Forum Security and interoperability
  - Common discussions
- Ongoing work within the STM-community
  - Common standardization work: S-124, S-421, SECOM, General STM news

4) Overview on Navelink usage

2023-11-30





Events since last Dev Forum:

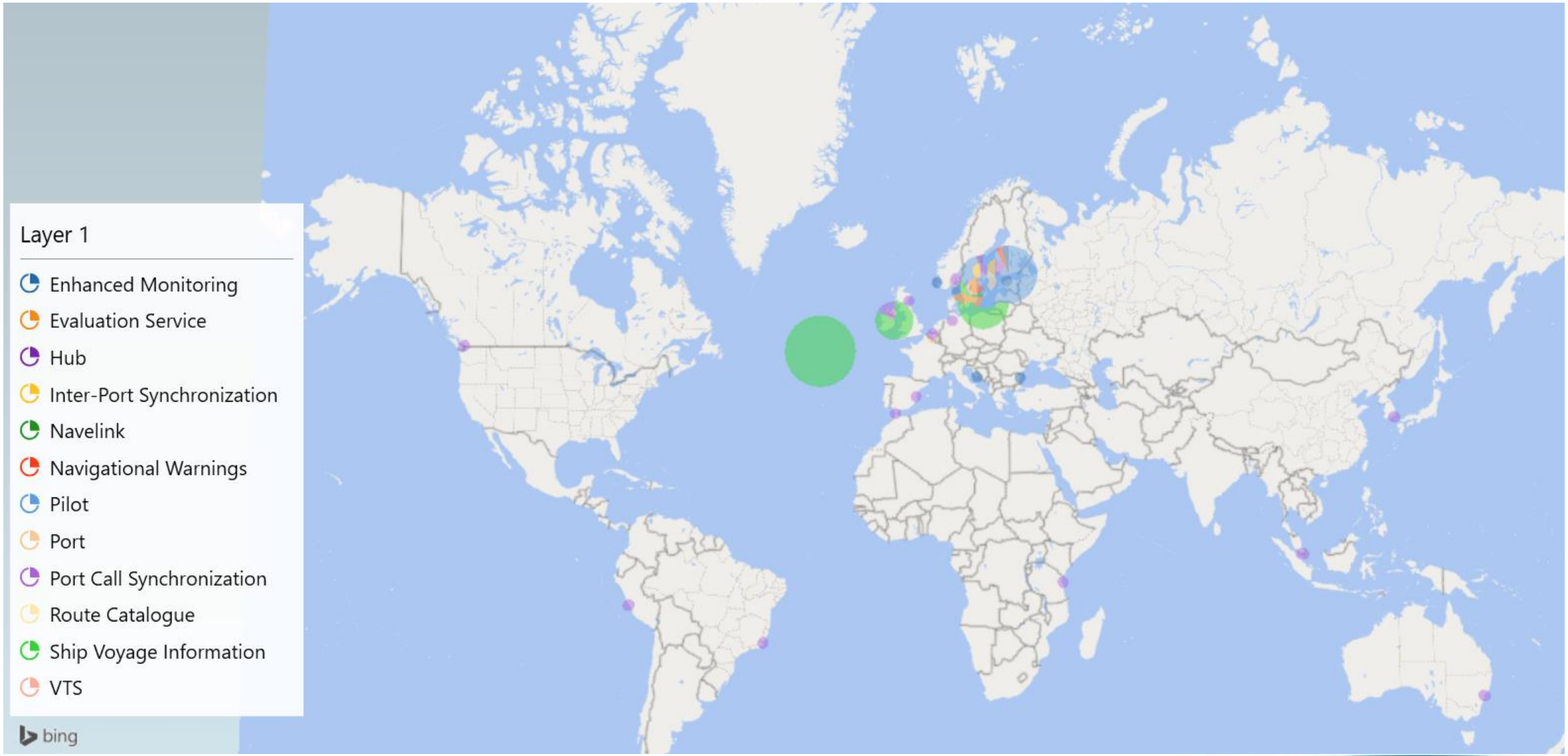
2 ships in OPS
Services in DEV

Navelink Operational environment Service Registrations

Service Specifications: 1 (Voyage Information Service v2.2)
Service Technical Design: 1 (Voyage Information Service Design v2.2)
Service Instances: 173

NAVELINK

Operational environment



NAVELINK

5) Q&A

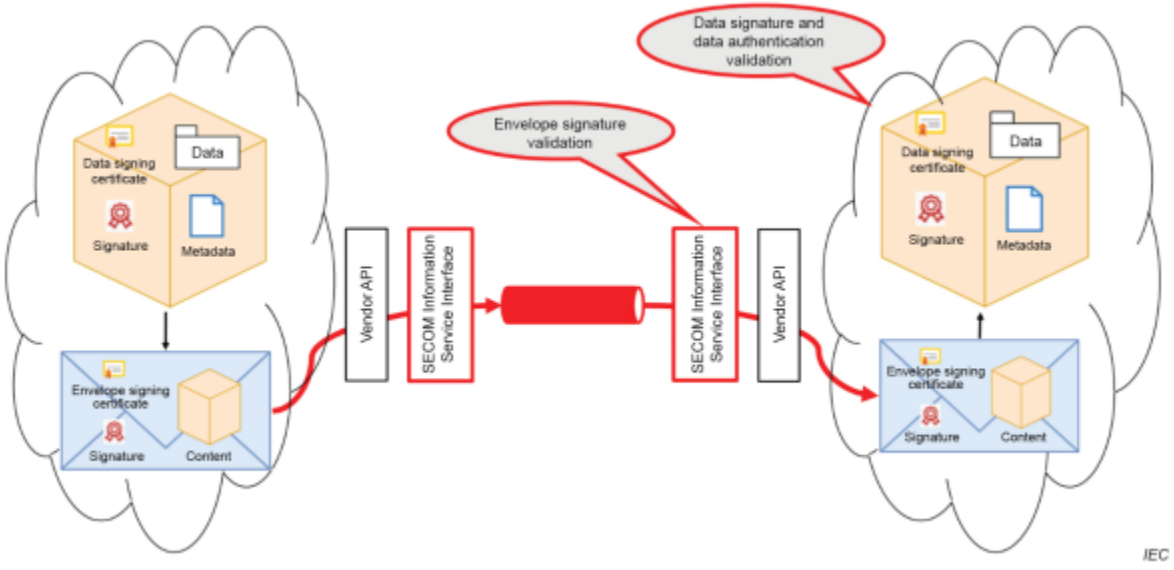
- Any Questions? The floor is open.

6) Demo

- How to Implement SECOM Upload interface by Mikael Olofsson (Navelink)

Reference: IEC 63173-2:2022 | IEC Webstore
IEC 63173-2 SECOM Clause 5 SECOM Service interface

IEC 63173-2 SECOM (cirm.org) (https://cirm.org/secom/)
SECOM - STM – Sea Traffic Management (https://www.seatrafficmanagement.info/developers-forum/secom/)



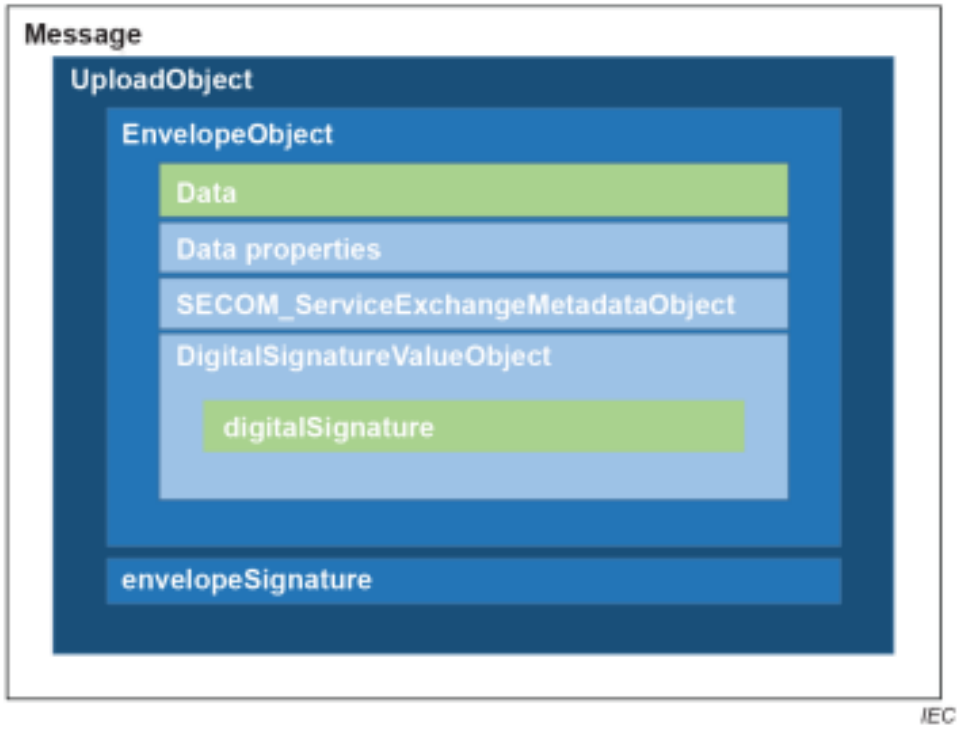
Interface	Comment
Upload	This interface is called when client uploads (pushes) data to the service. The sender (client) decides format and protection of the data.
Upload Link	This interface is called when client uploads (pushes) a reference pointer to large data. The data is downloaded using interface Get By Link.
Acknowledgement	This interface is called as response to Acknowledgement request in Upload.
Get	This interface is called when client gets (pulls) data from the service.
Get Summary	This interface is called when client gets a summary of available data from the service. The data is retrieved (pulled) using the interface Get.
Get By Link	This interface is called when client downloads (pulls) large data by reference given from interface Upload Link.
Access	This interface is called when client asks for access to data from the service. Response is given by callback to Access Notification.
Access Notification	This interface is called as response to interface Access.
Subscription	This interface is called when client or server initiates subscription on data from the service. Response is given with interface Upload and Subscription Notification.
Remove Subscription	This interface is called when client or server removes subscription. Response is given with interface Subscription Notification.
Subscription Notification	This interface is called as response from Subscription or Remove Subscription.
Capability	This interface is called when client asks for the service capabilities.
Ping	This interface is called when client checks the availability of the service.
EncryptionKey	This interface is called when sending (pushing) encryption key to a receiver.
PublicKey	This interface is called when client gets (pulls) the public certificate(s) from the service.

NAVELINK

UPLOAD

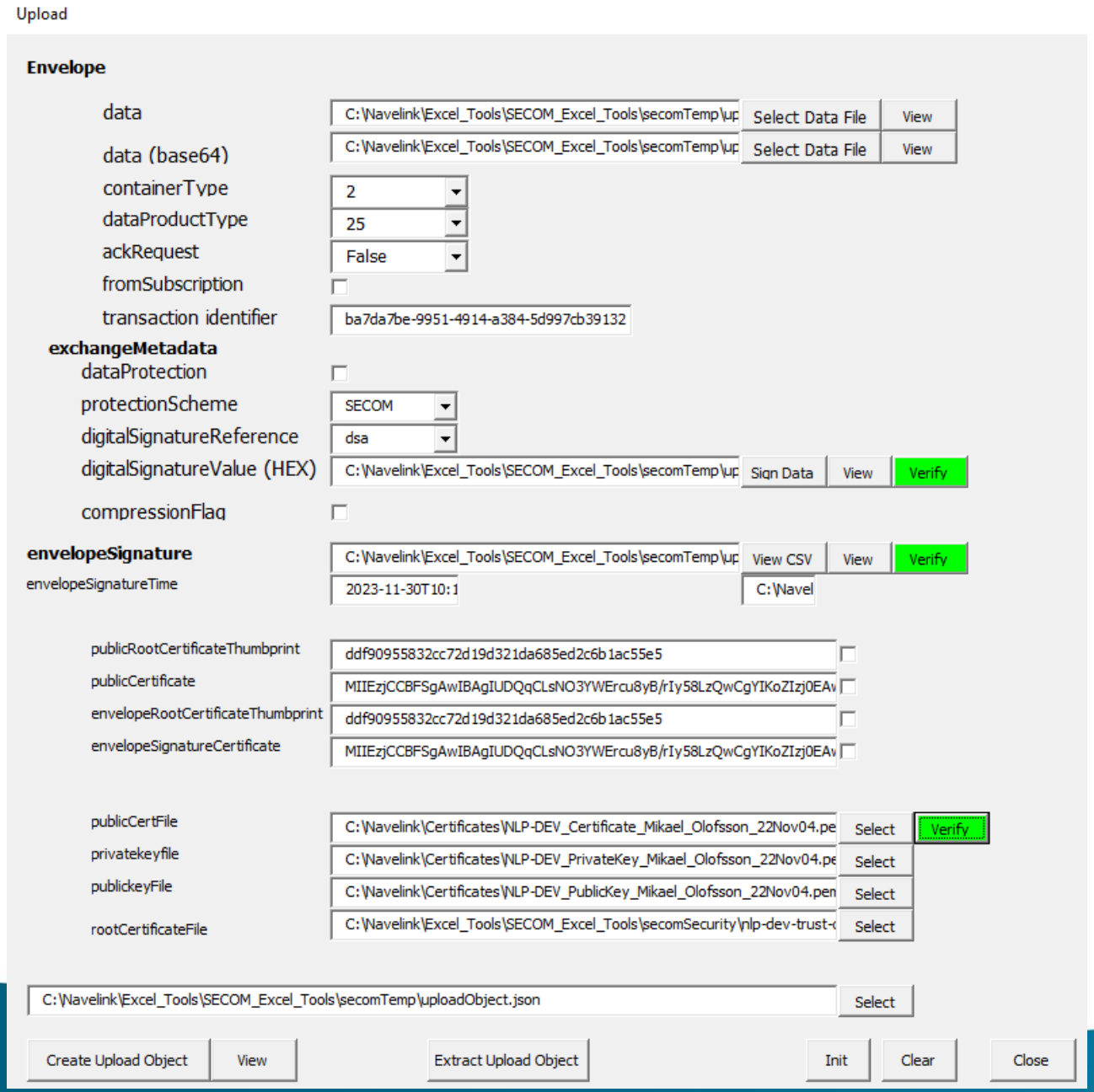
POST baseUrl/v1/object {body} : response

This interface is called when client uploads (pushes) data to the service. The sender (client) decides format and protection of the data. If acknowledgement is requested it will be given by callback to interface Acknowledgement.



Attribute	Type	Format	Require
envelope data	string	Base64	Required
envelope containerType	integer	enum	Required
envelope dataProductType	integer	enum	Required
envelope exchangeMetadata dataProtection	boolean		Required
envelope exchangeMetadata protectionScheme	string		Required
envelope exchangeMetadata dataSignatureReference	string		Required
envelope exchangeMetadata dataSignatureValue publicRootCertificateThumbprint	string	SHA1 and HEX	Optional
envelope exchangeMetadata dataSignatureValue publicCertificate	string	Minified PEM	Required
envelope exchangeMetadata compressionFlag	boolean		Required
envelope fromSubscription	boolean		Optional
envelope ackRequest	boolean		Required
envelope transactionIdentifier	string	uuid	Required
envelope envelopeSignatureCertificate	string	Minified PEM	Required
envelope envelopeRootCertificateThumbprint	string	SHA1 and HEX	Optional
envelope envelopeSignatureTime	string	date-time	Optional
envelopeSignature	string	HEX	Required

Example



1. INTERPRETATION GUIDELINES

The data is always provided in one line Base64 encoded string.
The data content is defined by

- Type of message in dataProductType [enum] as integer
  e.g. 24 = S-421
- Wrapping according to containerType [enum] as integer
  e.g. S-100 DataSet
- ZIP according to compressionFlag
- Encrypted according to dataProtection [flag]
  True means data is encrypted and a encryptionKey is needed

Data signature shall be provided in one line HEX format using DSA (**dataSignatureReference**).

The name of the **protectionScheme** is not specified by SECOM and need to be agreed upon. The proposal here is to use SECOM but may need to be more specified, e.g. Navelink SECOM.

Exchange information

- Transaction identifier in UUID (unique for every upload)
- Standalone or in subscription according to fromSubscription [flag]
- Acknowledgement request according to ackRequest

Envelope signature

The envelope signature shall be made on a dot (.) separated “CSV” data structure of the envelope:
data (Base64).containerType (int).dataProductType (int).dataProtection (true/false).protectionScheme (String).publicRootCertificateThumbprint .publicCertificate (Base64 minified PEM).digitalSignature (one line HEX).compressionFlag (true/false).fromSubscription (true/false).ackrequest (int).transactionidentifier (String UUID).envelopeSignatureCertificate (Base64 minified PEM).envelopeRootCertificateThumbprint.envelopeSignatureTime (UNIX seconds)

NAVELINK

UploadObject in JSON


```
{
"envelope": {
"data": ”<base64>",
"containerType": 2,
"dataProductType": 25,
"exchangeMetadata": {
"dataProtection": false,
"protectionScheme":"SECOM",
"digitalSignatureReference":"dsa",
"digitalSignatureValue": {
"publicRootCertificateThumbprint": "93ca5fce76d8622187b3f39375694e623eb73e97",
"publicCertificate": ”<cert>",
"digitalSignature":
"3065023100941202D55C0795310B98C8FA691A168A72E337E04045B0E15BF215564FBC589EC7A7772AD836F642BFD5EC219F320CA402304AD2
776461D540572AF793CABE25B0AFFFE6FC07677308D307305DFF868EA3735FE98A7747D99A2877B8FEB627B8D779"
},
"compressionFlag": false
},
"fromSubscription": false,
"ackRequest": 0,
"transactionIdentifier": "ba7da7be-9951-4914-a384-5d997cb39132",
"envelopeSignatureCertificate":”<cert>",
"envelopeRootCertificateThumbprint": "93ca5fce76d8622187b3f39375694e623eb73e97",
"envelopeSignatureTime": "2023-11-30T10:19:41"
},
"envelopeSignature":"3065023100AC2ECE2427C3D967611D838C2E7D50EE18427D5749021CB7513683F5E98DF0BE6228A07807E1E22884D2B72
CF5F59E1002303163EE49B12F04FBB5D9DB2436F9B2CDAAE19A3BEAE48FA19A3B5334A315CBABB25E8560EF2D14CDA59338791BBF1158"
}
```

Enums

5.6.7 SECOM_DataProductType

Table 8 contains the supported product types used in SECOM information interfaces 5.7.5, 5.7.6, 5.7.8, 5.7.10 and 5.7.13.

Table 8 – SECOM_DataProductType

SECOM_DataProductType	
Name	**Description**
OTHER	Other data types not covered in this table
S57	S-57 Electronic Navigational Chart (ENC)
S101	S-101 Electronic Navigational Chart (ENC)
S102	S-102 Bathymetric Surface
S104	S-104 Water Level Information for Surface Navigation
S111	S-111 Surface Currents
S122	S-122 Marine Protected Areas (MPAs)
S123	S-123 Marine Radio Services
S124	S-124 Navigational Warnings
S125	S-125 Marine Navigational Services
S126	S-126 Marine Physical Environment
S127	S-127 Marine Traffic Management
S128	S-128 Catalogue of Nautical Products
S129	S-129 Under Keel Clearance Management (UKCM)
S131	S-131 Marine Harbour Infrastructure
S210	S-210 Inter-VTS Exchange Format
S211	S-211 Port Call Message Format
S212	S-212 VTS Digital Information Service
S401	S-401 Inland ENC
S402	S-402 Bathymetric Contour Overlay for Inland ENC
S411	S-411 Sea Ice Information
S412	S-412 Weather Overlay
S413	S-413 Marine Weather Conditions
S414	S-414 Marine Weather Observations
S421	S-421 Route Plan
RTZ	Route Plan
EPC	Electronic Port Clearance

Table 10 – AckRequest Enum

AckRequestEnum	
Value	**Definition**
0 (default)	No ACK requested
1	Delivered ACK requested
2	Opened ACK requested
3	Delivered + Opened ACK requested

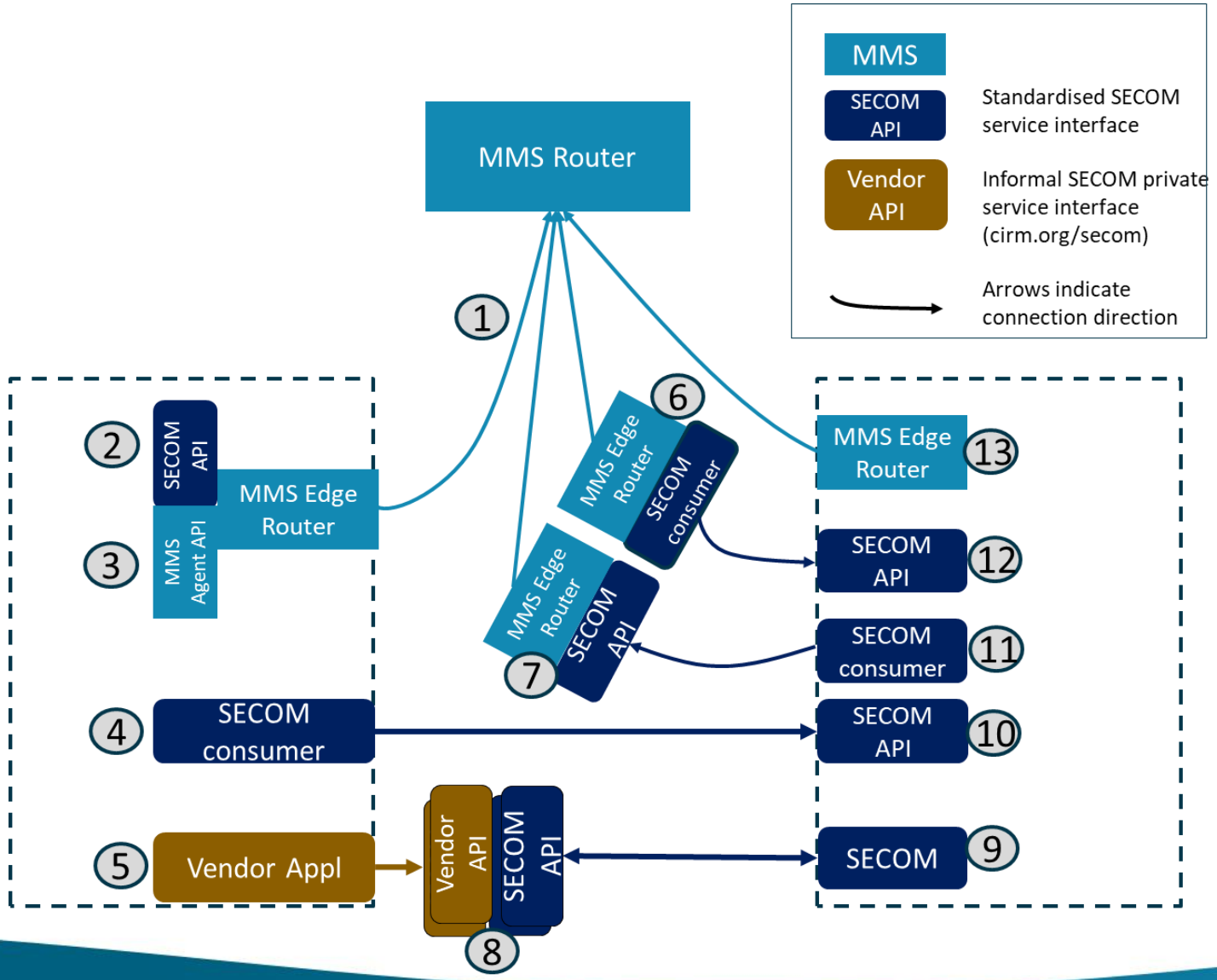
Table 7 – ContainerTypeEnum

ContainerTypeEnum	
Value	**Definition**
0	S100_DataSet
1	S100_ExchangeSet
2	NONE

S-100 ed5

Value	RSA	1	RSA with key length >= 2048 bits
Value	DSA	2	DSA with key length >= 2048 bits
Value	ECDSA	3	ECDSA with key length >= 224 bits.
Value	ECDSA-224-SHA2-224	4	224 bits ECDSA with SHA2-224 hashing
Value	ECDSA-224-SHA3-224	5	224 bits ECDSA with SHA3-224 hashing
Value	ECDSA-256-SHA2-256	6	256 bits ECDSA: SHA2-256
Value	ECDSA-256-SHA3-256	7	256 bits ECDSA: SHA3-256
Value	ECDSA-384-SHA2	8	384 bits ECDSA: SHA2-384
Value	ECDSA-384-SHA3	9	384 bits ECDSA: SHA3-384
Value	AES-128	10	AES 128 bit keys
Value	AES-192	11	AES 192 bit keys
Value	AES-256	12	AES 256 bit keys

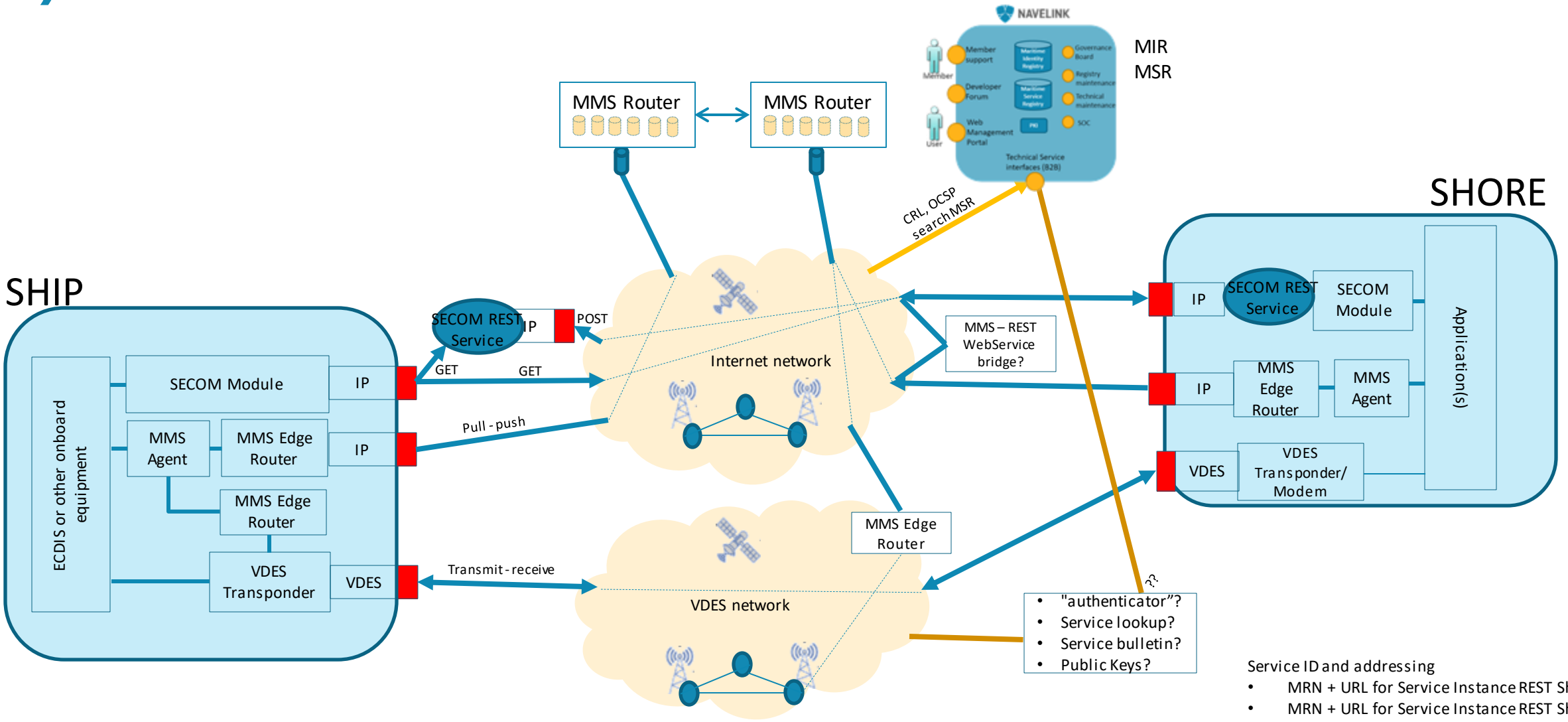
MMS – SECOM integrations points



1. MMS network can be either internet or VDES
2. SECOM API as user front to MMS
3. MMS Agent interface as user front
4. SECOM consumer calling other SECOM service
5. Vendor application as user front to SECOM service. Also called the SECOM private side. Can be either based on informal private API or existnig communication between e.g. ship and fleet operation.
6. Bridge from MMS to SECOM service
7. Bridge from SECOM service to MMS
8. SECOM service hosted by ”anyone” with a private side (vendor API) and the public side (the standard API)
9. SECOM Service and application allowing both outgoing and incomin calls to SECOM Service.
10. SECOM Service allowing incoming calls
11. SECOM consumer application
12. SECOM Service allowing incoming calls
13. MMS

NAVELINK

7) Discussion: Navelink + REST + MMS + VDES



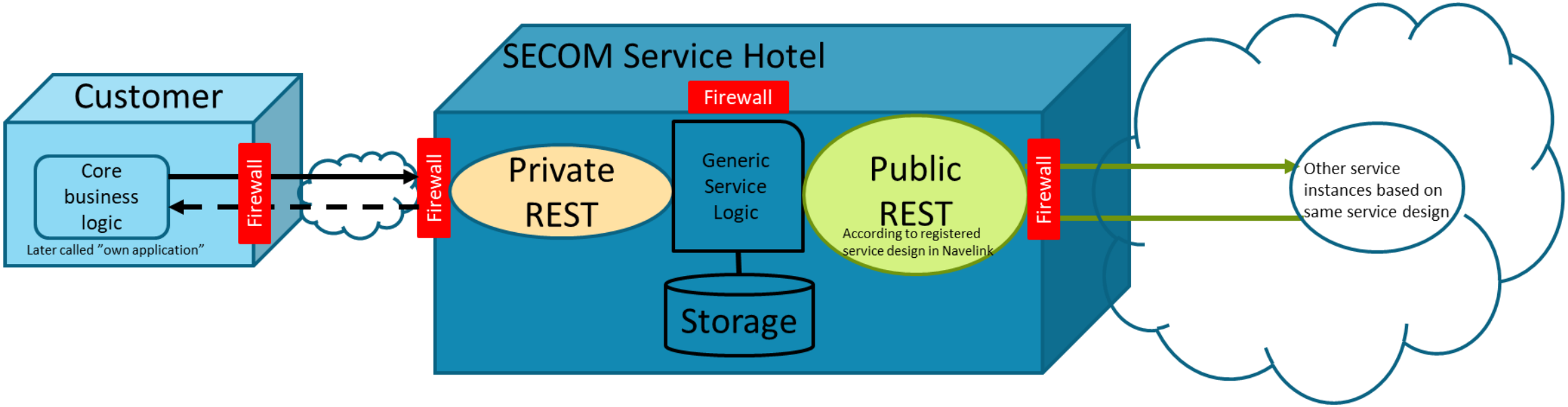
Service ID and addressing

- MRN + URL for Service Instance REST Ship
- MRN + URL for Service Instance REST Shore
- MRN for MMS Queue Ship
- MRN for MMS Queue Shore
- MRN + URL for MMS Router

NAVELINK

Introduction

The main purpose with the SECOM Service Hotel is to provide customers with REST Services compliant with the IEC standard 63173-2 SECOM. Navelink will host the services on behalf of the customers, and the customers applications connects to the private REST service. Other consumers will the connect to the SECOM Public REST service.



8) Closing remarks

- Next Developer Forum at 25/01-2024
  - Presentation on the topic "To design and implement SECOM Services, e.g. Service for S125 Aids to Navigate" by Nikolaos Vastardis (GLA)
- Happy Holidays!

Meeting notes

- Ongoing work with the SECOM Hotel development (Navelink)
  - To complement the VIS Hotel STM Services/ Give the option to users to move on to SECOM services instead. (See slide 14 for more details)
  - The client as information owner decides how to sign the data, type of data etc. The service signs the envelope and sends to data.
  - Questions and discussions about certificates is also ongoing as a result of the development
- Ongoing work with the SECOM technical design documents
- SECOM generic technical design can be found on Navelink MSR. There will be SECOM test services in the future as well to use
- Demo on How to Implement SECOM Upload Interface by Mikael Olofsson (Navelink)
  - Definition of SECOM Service interface is well described and standardised and can be used today
  - SECOM Upload interface to pushes data to another SECOM Service. Upload objects are created in json and wrapped in a signed envelope (see slide 10)
  - There are a lot of steps to produce the envelope (for example see slide 11)
    - SECOM Upload is independent of type of payload. Basically it is a base64 string that can contain “anything”, including ZIP file.
  - The idea of the template is based on that it should provide developers with all the steps necessary to provide its data through a SECOM service
  - MCC MMS working group is ongoing to define the MMS standard for the RTCM standardization group
- Next meeting 2024-01-25
  - Presentation on the topic "To design and implement SECOM Services, e.g. Service for S125 Aids to Navigate" by Nikolaos Vastardis (GLA)

NAVELINK

Navelink.org