SECOM 1

Architecture & PKI

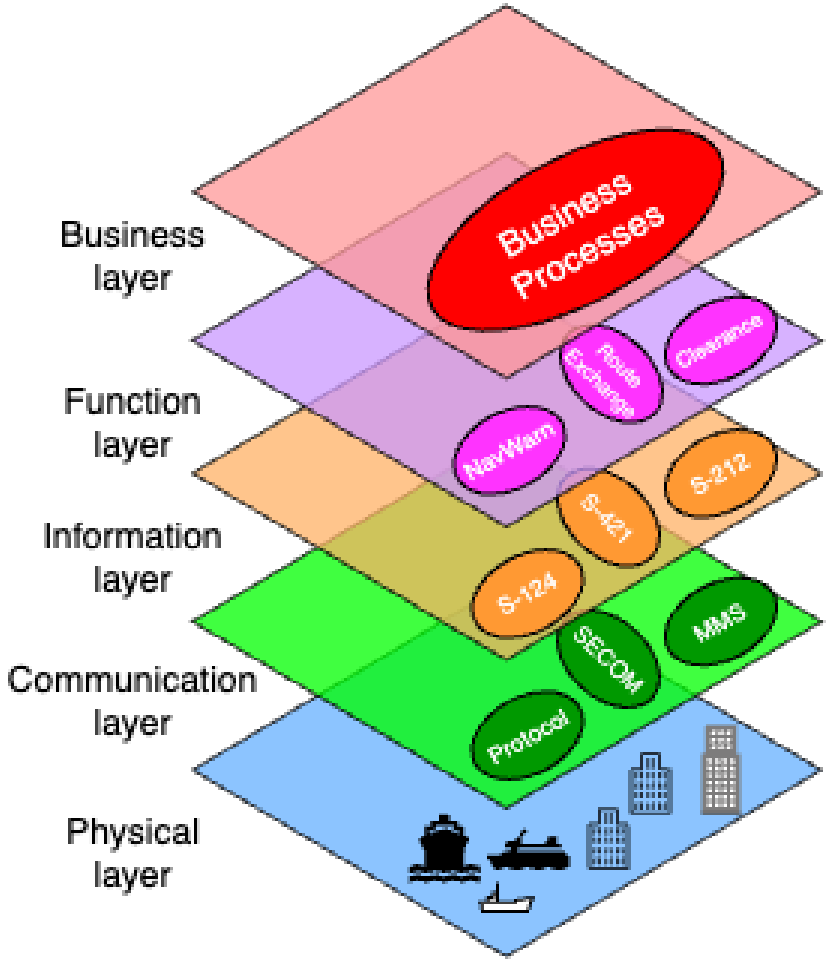
SOLITA

What is SECOM?

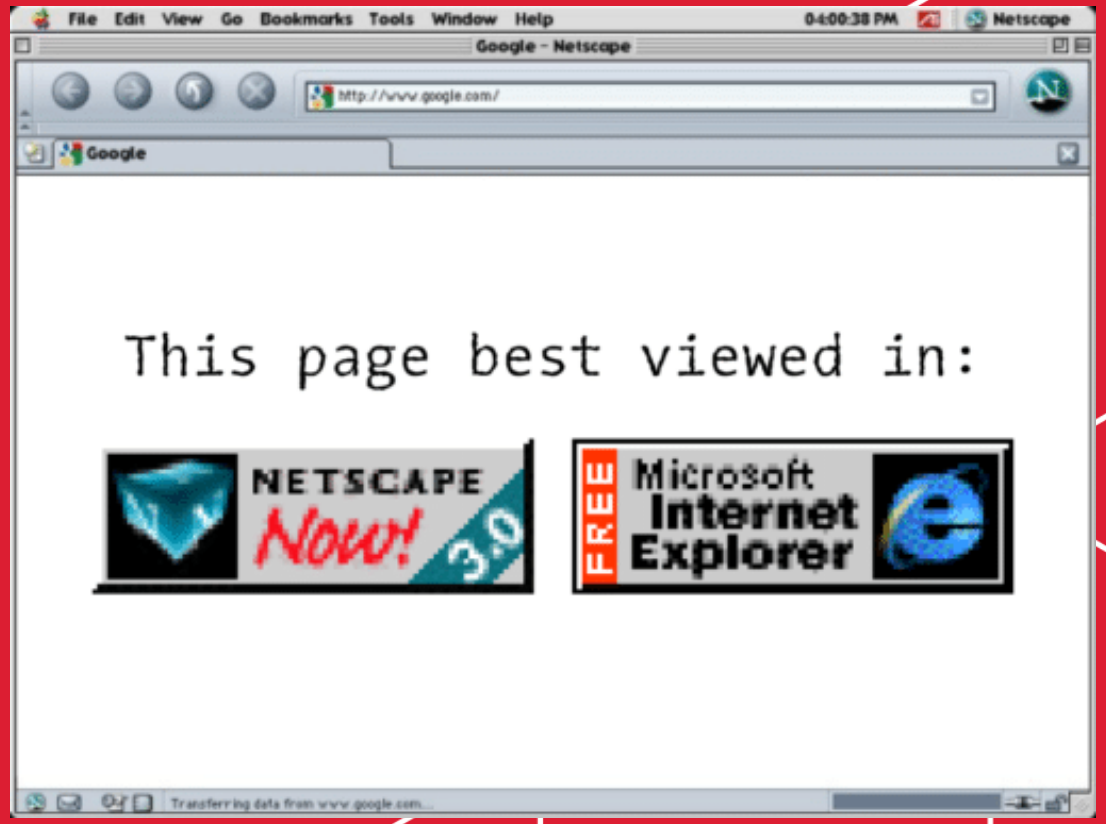
- SEcure COMmunications between ship and shore, IEC 63173-2
- Basically
  - REST APIs
  - Authenticity, encryption, compression and interactions between actors defined
- Looks complicated at first, but there is a reason for that
- A *building block* to help the developers of digital services and their consumers in the maritime sector

So, what is SECOM?

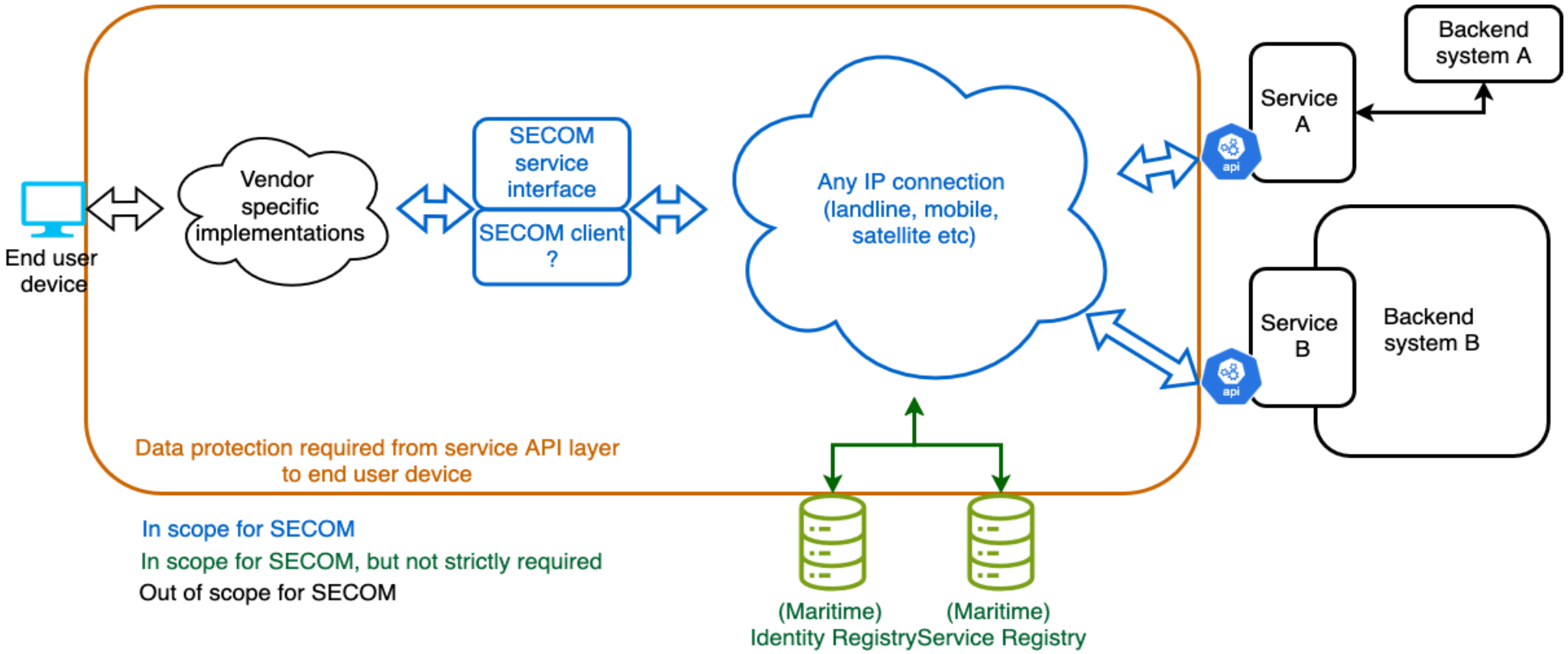
- Standard set of REST APIs that define interactions between services and their consumers
- Data agnostic
  - SECOM APIs work with JSON
  - Data payload is base64 encoded
- All communication is secured (TLS)
- All communication is signed
- Supports payload encryption



Remember the browser wars?



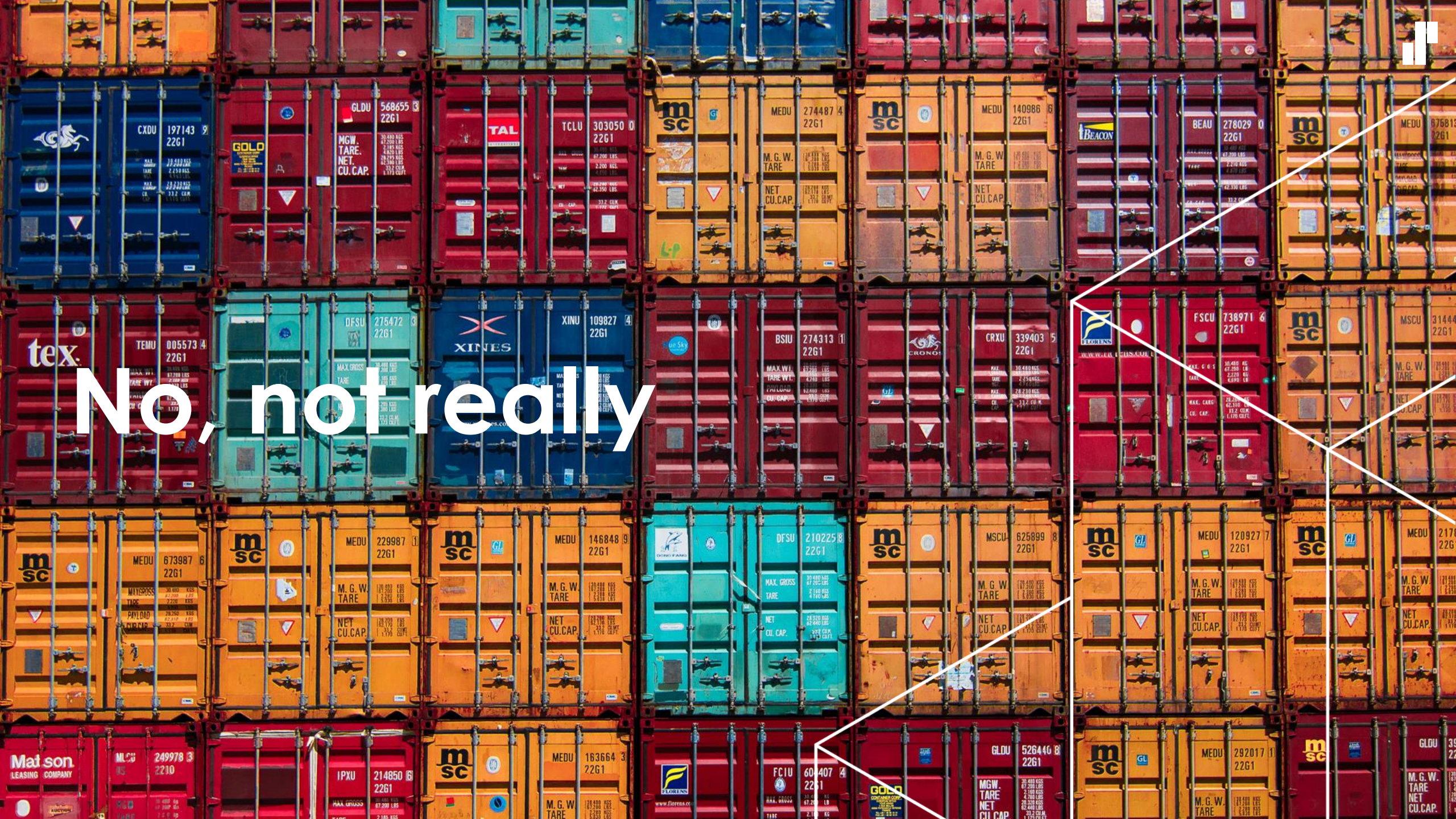
Architecture



Definitions

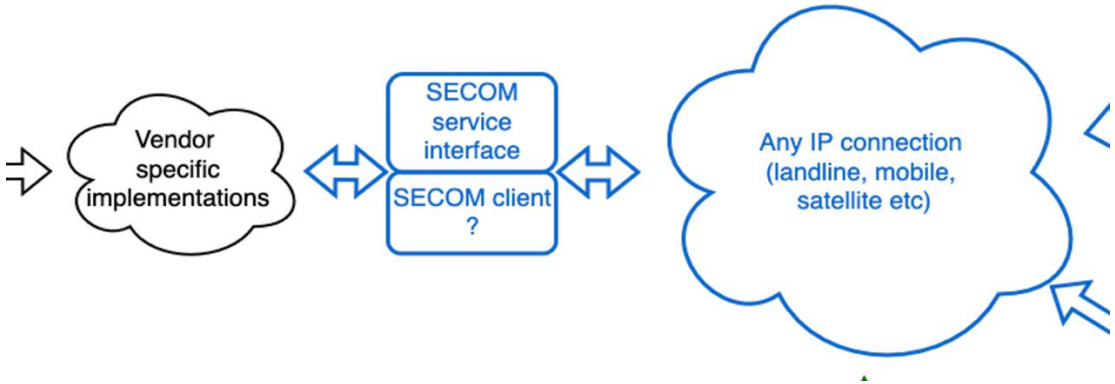
- Service – a shore side system providing a service for consumers, e.g. route exchange service. Typically integrated with or a component of back-end systems, e.g. a VTS system.
- Consumer – a system using the service, e.g. ship systems (including ECDIS) that use the route exchange system
- Server – HTTP server that is provided by both service and consumer
- Client – HTTP client that is used to create HTTP calls from service and consumer
- Last-mile – The communication link between shore server of consumer and the ship systems

SECOM is complicated


No, not really

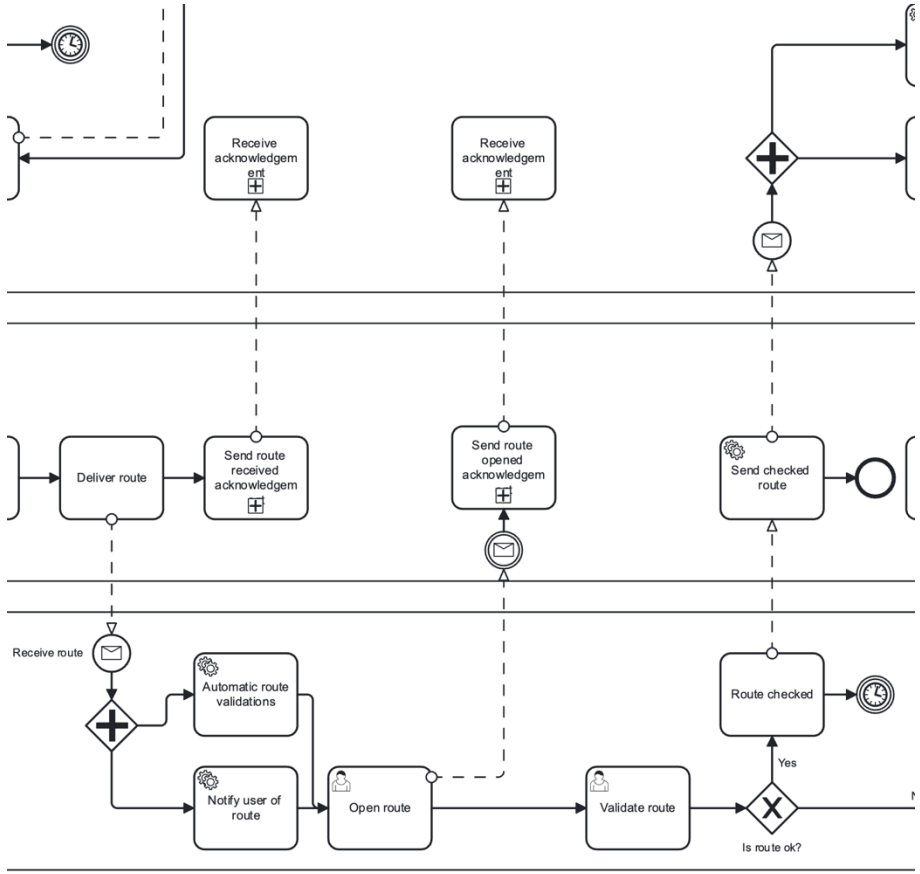
It has to support communication via poor connectivity

- Consumer's server may be on land to have a more stable connection
- Data compression is a part of the defined API (ZIP)



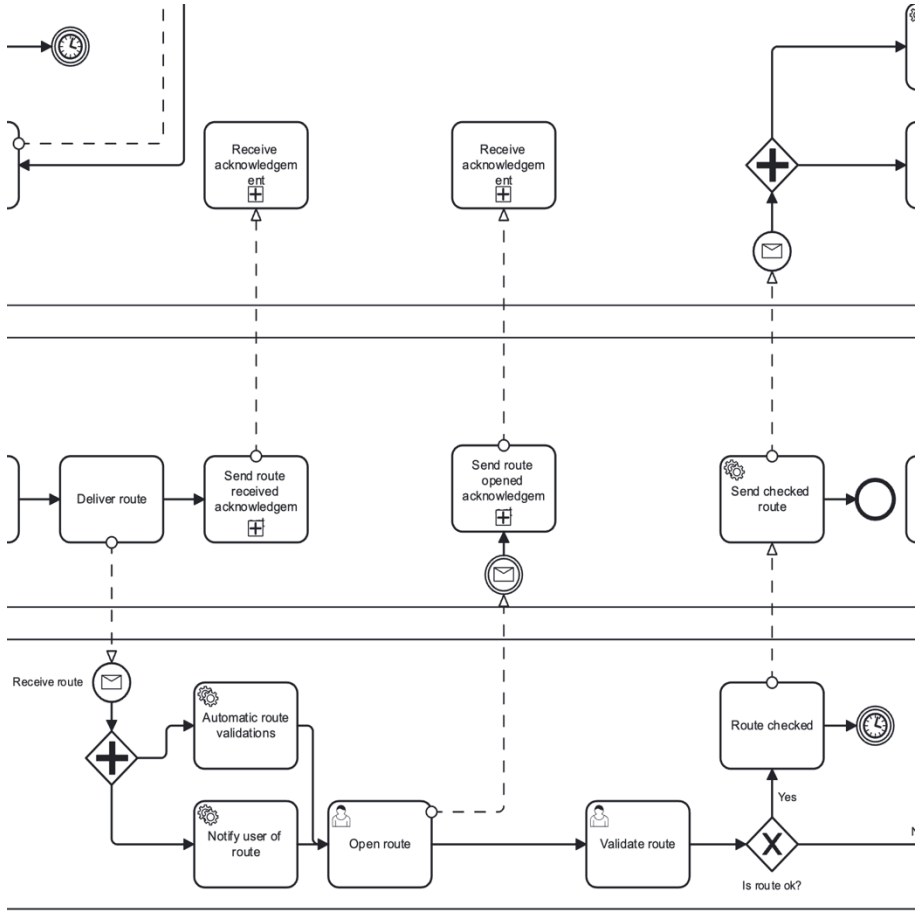
It has to support asynchronous processes

- HTTP client and server on both sides
- Websockets will not work
  - See previous slide
  - Many business processes require human interaction and are not that time critical



It has to support closed loop communication

- A technical ACK at the end of the HTTP/TCP connection is not enough
- Acknowledgment interface to the rescue
  - Delivery
  - Opened
- The definition of opened is up to interpretation

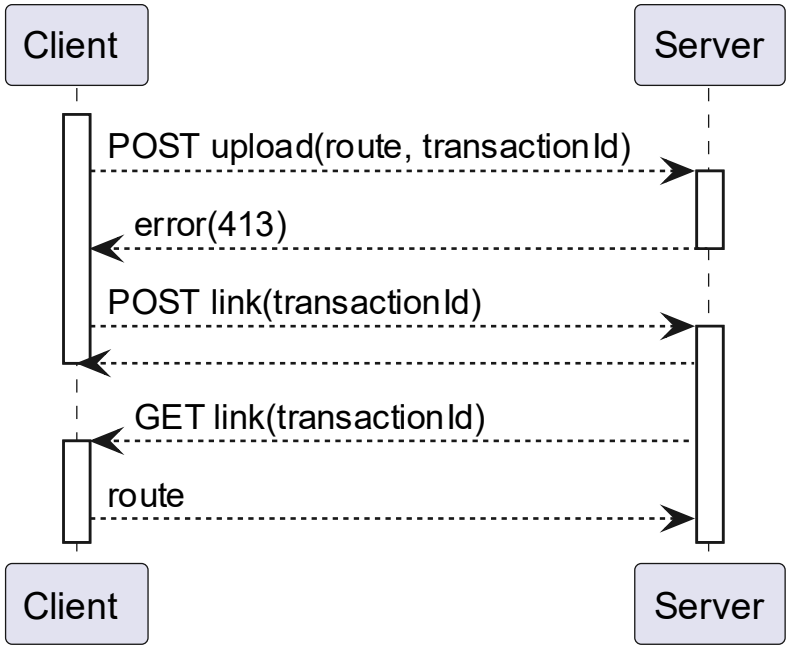


It has to support payload encryption

- Because there are intermediate steps that may not be trusted
- Interfaces exist to exchange one-time secrets between service and consumer to ensure end-to-end payload encryption

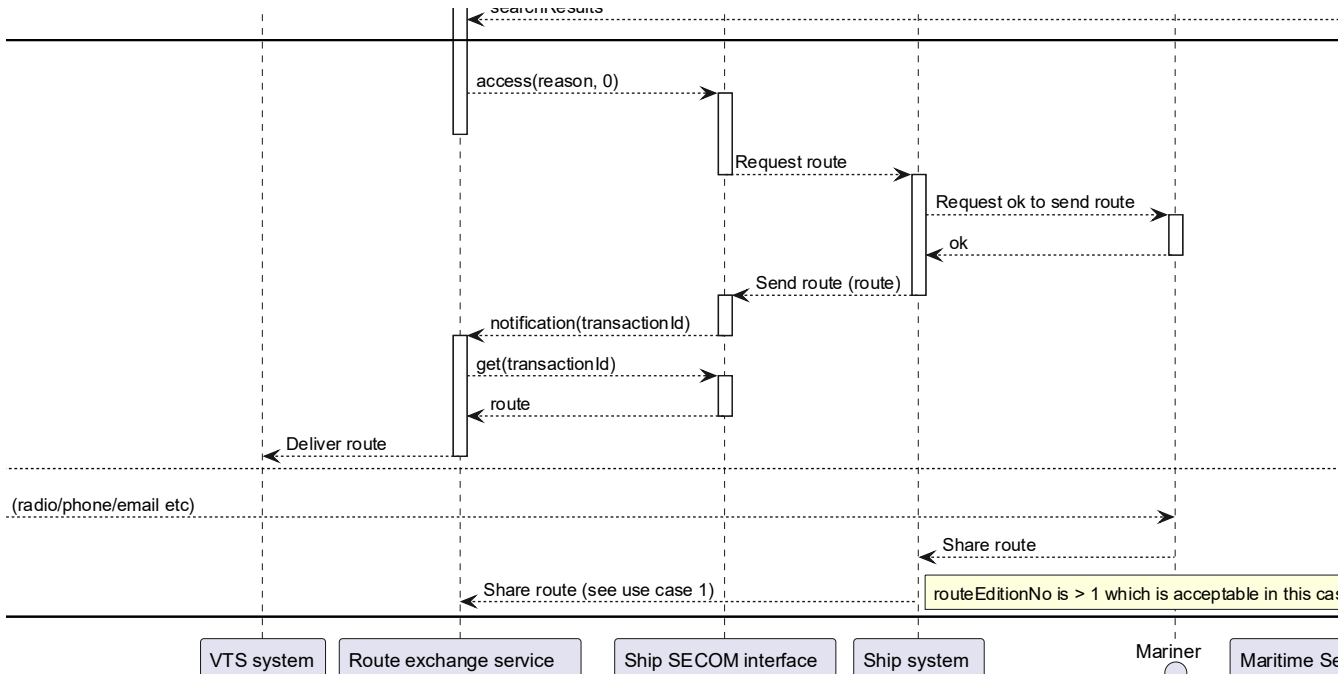
It has to support POSTing large payloads

- HTTP has no standard of max size for POSTs
- As most payload is text, compression may just save you



It has to support requesting access ascynchronously

- Granting or denying access on a case by case basis is possible
- Use cases for this need may be rare



PKI (Public Key Infrastructure)

- Standard X.509 certificates
- G1183 defines additional fields to adopt approach better to maritime domain
- SECOM v1 supported mTLS
- SECOM v2 dropping support for mTLS and certificates delivered as part of SECOM headers in all requests
- SECOM envelope and payload may have different signing entities


What is missing?

- Rev 2 will update all algorithms to modern versions and allow for updating algorithms as recommendations change
- Rev 2 removes dependencies on consumers being registered in service registries
- SECOM does not define retries if a call fails
- SECOM does not define the business process around a service
  - Service Specifications and Service Designs do this when specified according to IALA G1128

Future and timelines

- Rev 2 in under work by IEC TC80 WG17
  - Recommend to begin implementing against Rev 2
- Timeline currently to get final version published late 2026/yearly 2027

Thank you!

Ramin Miraftabi
Senior Consultant
+358 50 563 2485
ramin.miraftabi@solita.fi

Additional information

- IALA Technical Services https://www.iala.int/technical/technical-services/
  - G1128
  - G1183
  - G1191
  - Service Specification for Route Exchange
  - Service Design for Route Exchange
- SECOM test data https://cirm.org/secom (version 1 currently)