NAVELINK

Developer forum

25-01-2024

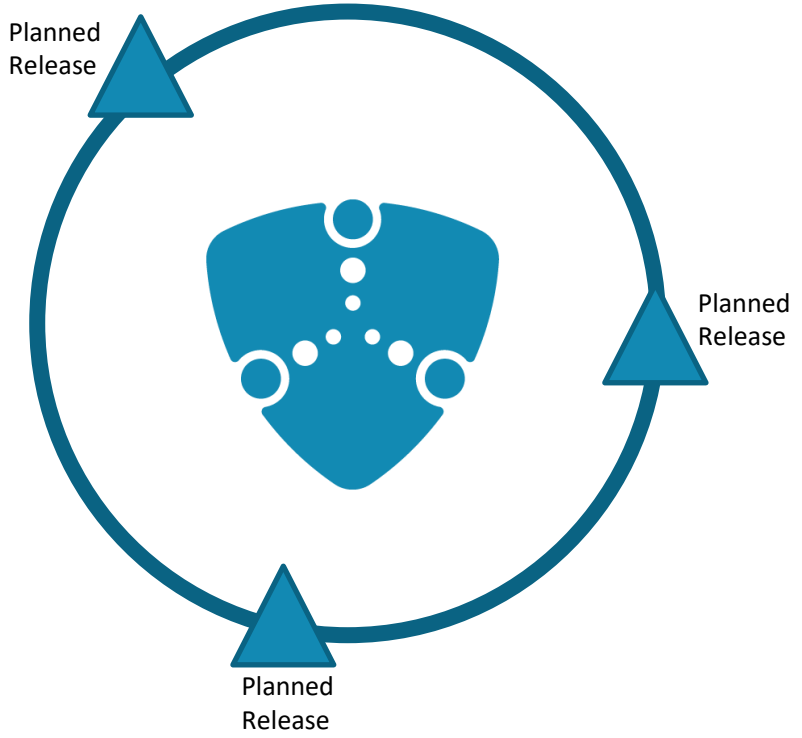
Navelink.org

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)
4) Overview of Navelink usage
5) Q&A
   a) New questions (All)
6) Presentation & Demo - S-125/S-201 e-Navigation services by Nikolaos Vastardis (R&D GLA UK & Ireland)
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
  - Implementation of MIR v.1.2.2 to DEV & TEST
- Future
  - Implementation of MIR v.1.2.2 to PROD
    - *Planned date for implementation next Friday, 02/02-2024*
  - Continued work with the creation of SECOM Hotel



Received questions

-

2) Navelink Roadmap

0-2 years

2-5 years

Add SECOM Hotel

Increase SECOM Compliance

Add MMS support

MRR

Future MSR

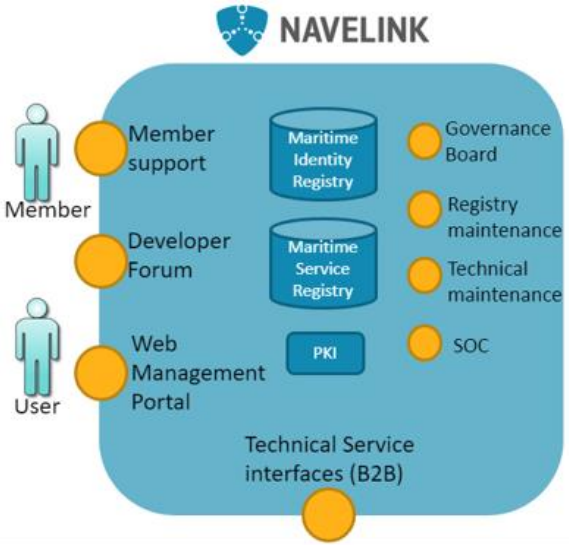
New Management Portal

Support new Service Specifications and Designs

Increase VDES support

Enable subscription on Navelink technical notes

Add support for Service Payment

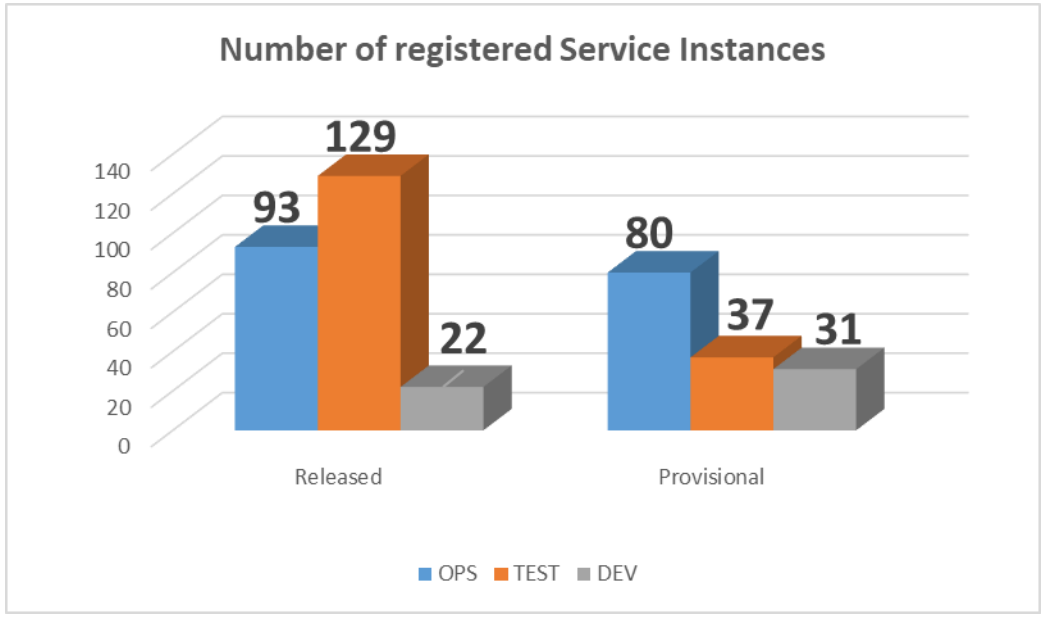


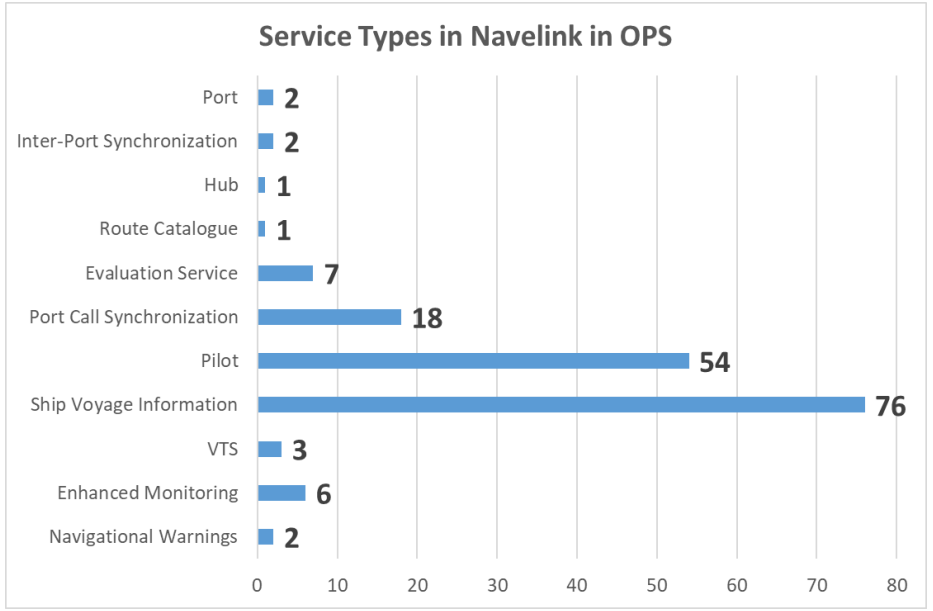
3) Service development discussions & information

- Forum service developers
  - Common discussions
  - PKI1.6 Every Identity Service Provider is to generate and publish CRLs containing any revoked MCP ID certificates for each of its issuing CA's. Considering the above, recommendations for certificate validity periods in a root-intermediate-client hierarchy are:
    - *MCP Instance/authority: Root-CA: 10 years validity and renewed every 3 years, start signing when 1 year old.*
    - *MCP Instance/authority: Intermediate-CA: 3 years validity, renew every 1 year, start signing when 1 year old.*
    - *End-system or client certificate (signed by intermediate): 6 months validity, renew 2 months before expiry.*
- Forum Security and interoperability
  - Common discussions

4) Overview on Navelink usage

2024-01-25





Events since last Dev Forum:

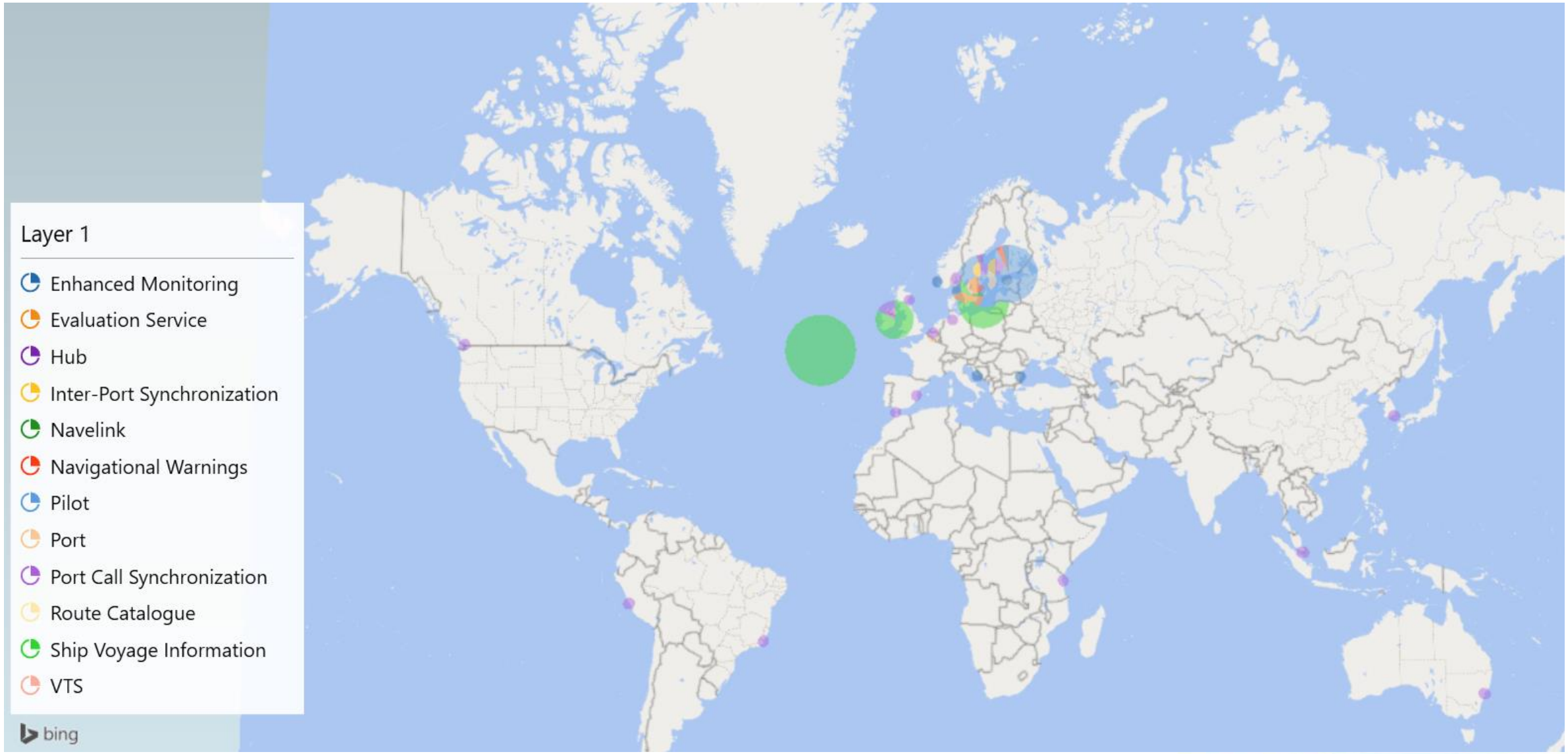
-

Navelink Operational environment Service Registrations

Service Specifications: 2 (Voyage Information Service v2.2) + **SECOM Generic Service Specification v1**
Service Technical Design: 2 (Voyage Information Service Design v2.2) + **SECOM Service Design Template v1**
Service Instances: 173

NAVELINK

Operational environment



5) Q&A

- Any Questions? The floor is open.

6) Presentation

- S-125/S-201 e-Navigation services by Nikolaos Vastardis (R&D GLA UK & Ireland)

GRAD Driving Innovation for Safer Maritime Navigation

GLA e-Navigation Service Architecture

Nikolaos Vastardis

January 2024

Introduction

- The e-Navigation concept was developed by the IMO and introduced in 2009 to improve safety and efficiency of navigation in the maritime domain.
- The General Lighthouse Authorities of UK and Ireland (GLA) are also planning for the implementation of e-Navigation and Maritime Digital Services.
- A number of potential use cases were identified with the transmission of Virtual AtoN (VAtoN) being one of the most noteworthy ones.
- This work introduces:
  - A novel prototype of an e-Navigation Service Architecture.
  - The way this integrates with the Maritime Connectivity Platform (MCP) for supporting SECOM operations.
  - A live VAtoN transmission using the implemented e-Navigation Demonstrator test-bed.

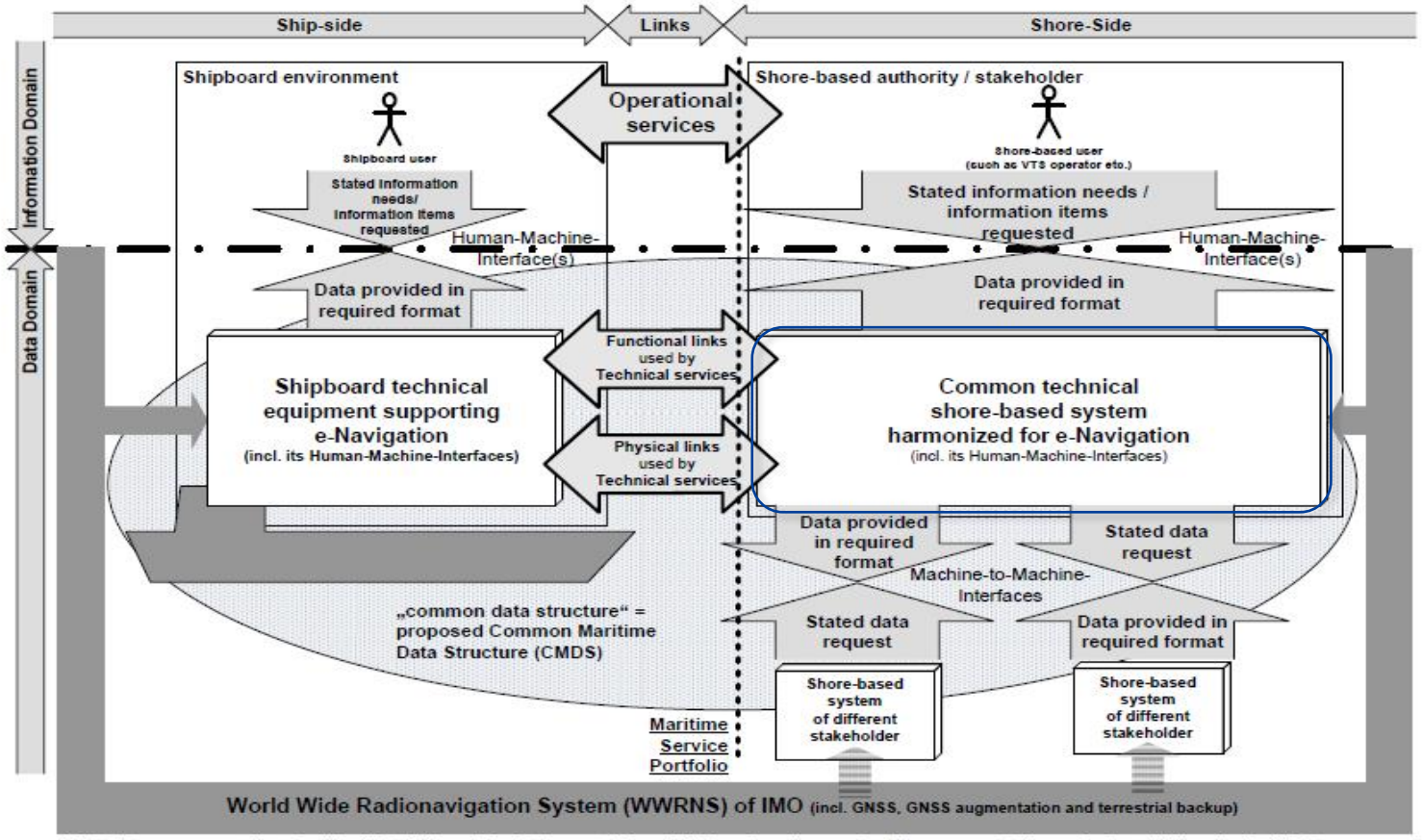
Background

The IMO provided an overview of its overarching e-Navigation architecture.

In response IALA published a number of guidelines e.g.:

- G1113 (Infrastructure Principles)
- G1114 (Infrastructure Specs)
- G1128 (Technical Service Specs)
- G1143 (MRN)

Specific focus was given on the Common Short-Based System Architecture (CSSA).



Note: There are operational and technical interactions between different shipboard environments. These are not shown for simplicity's sake in this figure.

Background – CSSA Technical Services

1. **The Data Collection and Data Transfer Services (DCT)**: A group of technical services interfacing the shore-based system via the physical links to traffic objects' electronic systems, to the waterways and to the natural environment.
2. **The Value-Added Data Processing Services (VAD)**: A group of individual technical services. Their main task is to add value to (raw) data by processing, combination, comparison etc.
3. **The User Interaction Service (UIA)**: An individual technical service specialised to provide the Human-Machine-Interface (HMI) to the primary users of the CSS.
4. **The Gateway Service (GWY)**: Another individual technical service specialised in data exchange shore-to-shore. It interfaces mainly to external systems of third parties.

Important Points:

- The CSSA is based on the Service Oriented Architecture (SOA).
- IEC (in coordination with IALA) developed SECOM for secure communication with the CSSA.

The GLA e-Navigation Architecture Design Process

- The design process followed:
  - Risk-Benefit Analysis of selected use cases
    - Ability to support VAtoN of great interest to the GLA
  - System Requirements capture:
    - Infrastructure level
    - Application level
  - Business Process Analysis (in parallel)
  - Architecture Design:
    - Microservice approach selected instead of pure-SOA
  - Service Identification:
    - DCT service for integrating with AIS/VDES + one for internal messaging
    - VAD service to store and distribute AtoN information (AtoN Service)
    - UIA service to interface with the users
    - GWY service to allow external access

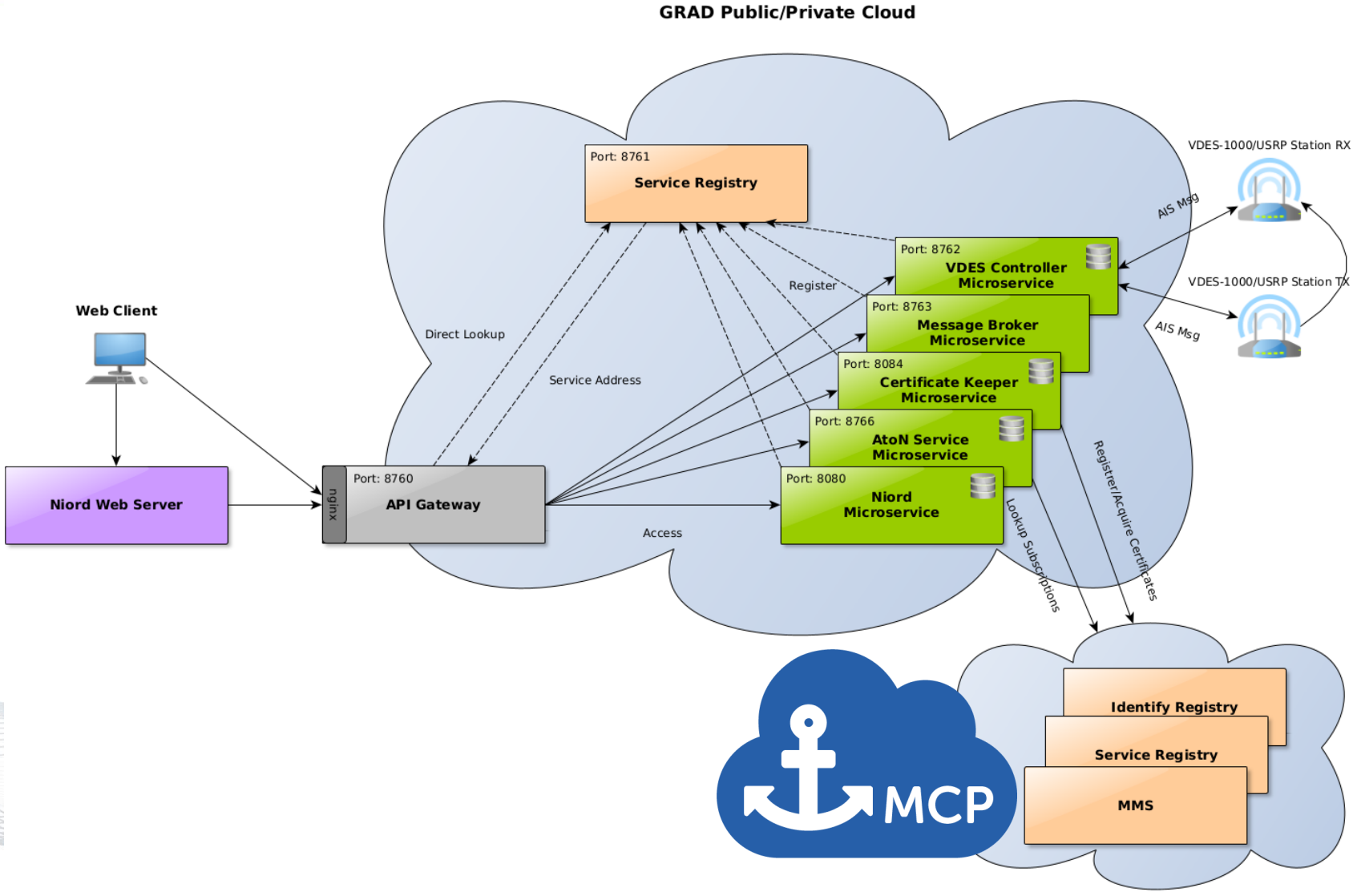
The GLA e-Navigation Architecture – MCP

- SECOM operations require a Public Key Infrastructure (PKI).
- MCP is an ideal a candidate to support the SECOM operations.
- Makes use of existing/emerging technologies like OpenID Connect, X.509 and MRN.
- It consists of:
  - Maritime Identity Registry
  - Maritime Service Registry
  - Maritime Messaging Service (in development)

An additional VAD service is needed to interface with the MCP.

- Signs and validates messages
- Handles MCP certificates (e.g., when expired)
- Simplifies the service implementations
- Can support other similar platforms

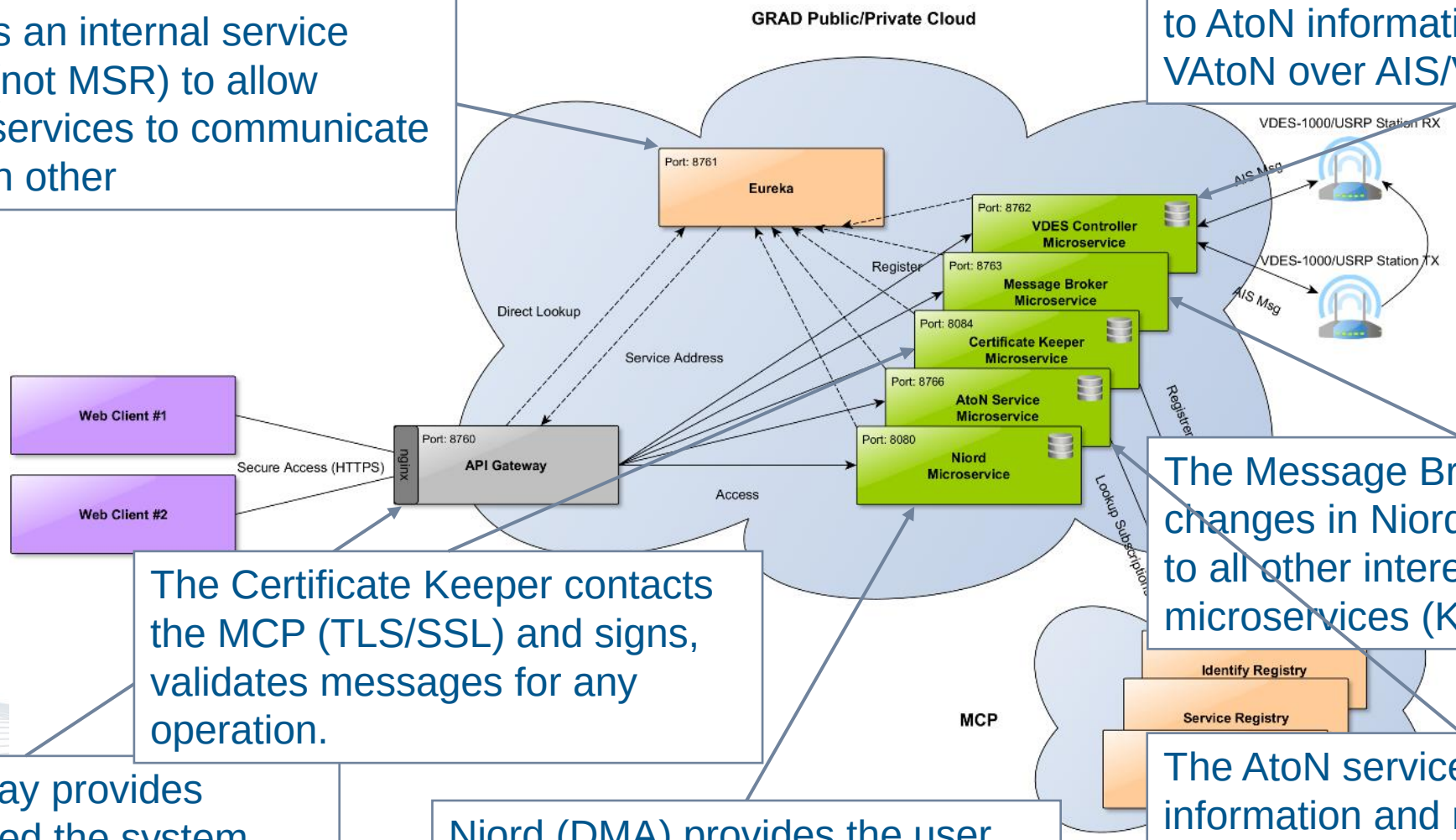
The GLA e-Navigation Architecture - Overview



The GLA e-Navigation Architecture - Overview

Eureka is an internal service registry (not MSR) to allow internal services to communicate with each other

VDES Controller polls/subscribes to AtoN information and transmits VAtoN over AIS/VDES.



The Message Broker allows changes in Niord to be published to all other interested microservices (Kafka).

The Certificate Keeper contacts the MCP (TLS/SSL) and signs, validates messages for any operation.

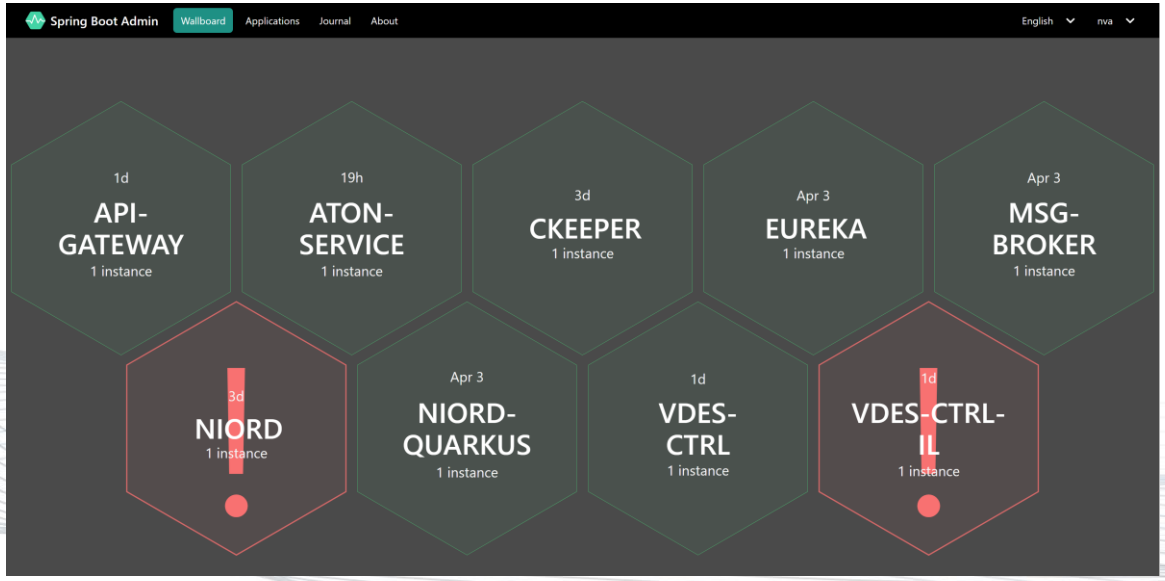
The API Gateway provides access, protected the system availability and also verifies SECOM requests.

Niord (DMA) provides the user interface for managing NW/NM and AtoN information.

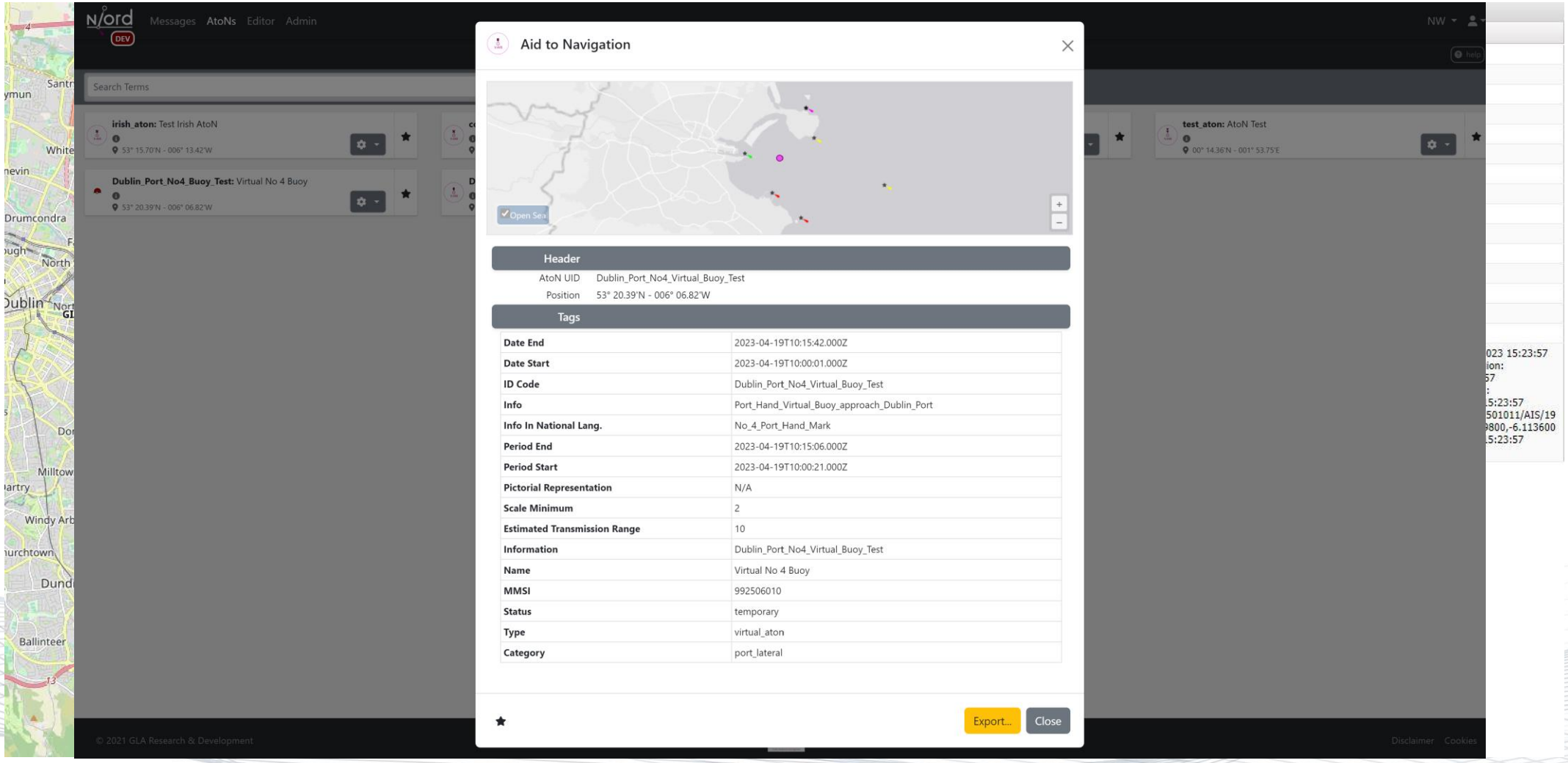
The AtoN service receives AtoN information and makes it available in S-125 format using SECOM.

e-Navigation Service Demonstrator

- An e-Navigation Service Demonstrator test-bed has been implemented and deployed in the GRAD premises.
- A CML VDES1000 module has been deployed by the Commissioners or Irish Lights (CIL) GLA in Ireland.
- Connectivity is achieved via a secure dedicated VPN.
- Data is encoded using a draft version (0.0.1) of S-125.



e-Navigation Service Demonstrator
VAtoN Transmission



Conclusion

- The GLA are developing a novel prototype e-Navigation Architecture for the provision of their future digital services.
- The design intends to follow all relevant maritime and industry standards.
- A microservice approach was deemed more appropriate instead of pure-SOA.
- The MCP is utilized to support the SECOM operations.
- An e-Navigation Service Demonstrator test-bed has been implemented by GRAD.
- Successful secure VAtoN transmissions using the test-bed has been performed.

The presented approach is intended to help not only the GLA but the maritime community as a whole.

Thank you!

Nikolaos Vastardis

Research & Innovation Engineer

Nikolaos.Vastardis@gla-rad.org

+44 (0) 7815 654897

8) Closing remarks

- Planned implementation of MIR v.1.2.2 to PROD the 02/02-2024
  - Release notes can be found at https://www.navelink.org
  - If you have any feedback about the update or want to move the implementation date further ahead, please contact us at info@navelink.org
- If you have any feedback regarding the change of the client certificates from 2 years validity to 6 months, what consequences do you have if this change occurs and what security concerns ect. do this raise? Again please contact us.
- Next Developer Forum at 22/02-2024

Meeting notes (1/2)

- MIR v.1.2.2. has been updated on DEV and TEST with planned implementation of MIR v.1.2.2 to PROD on 02/02-2024, if you want to delay this update, please contact us at info@navelink.org
- Navelink intend to update MSR SECOM Search interface for full SECOM compliance.
- There is a proposal for certificate validity times that would mean changes to current validity times of Navelink certificates. Most notable change would be the change of the client certificates from 2 years validity to 6 months.
  - Our question to you are what consequences do you see if this change implemented and what security concerns etc. do this raise? If you have any feedback about this, please contact us.
  - Responses:
    - *(SAAB/Peter Bergljung) 6 months is too short*
    - *(SAAB/Peter B) Proposal to investigate revocation of certificates via VDES.*
  - (Mikael) Navelink can check what amount of data is required for certificate renewal (CSR) and revocation, and revocation list (complete or delta)
  - (GLA/Nikos) It might depend on how many certificates is needed and how they are distributed. Would each ship have own certificates or one company certificate for all its ships? Would individual certificates be needed, that would mean hundreds of certificates that need to be updated every 2-4 months. Then they will also keep download the list of valid certificates so even offline they can check towards any entity they may encounter. And if a trip is long with limited connectivity this might be difficult.
  - (Mikael) Yes I agree the key management and what type of certificates needs to be discussed more.
  - (SAAB/Peter Tomsson) I think you need to have it on individual level and the problem will be how do we check what certificates has been revoked without online connection? There VDES might be an option.
  - (SAAB/Perter Bergljung) There is a lot of discussions about certificate in VDES right now and I think that there will be many certificates on each ship. It is a very complicated problem.
  - (Mikael) Yes and who to trust is another topic that is under discussion in MCP forums. As a side note MCP specifications are now moving to IALA specifications and working towards standardization.
- There is also a proposal of a procedure that if you have a client certificate that is valid for 6 months and renew the certificates every 2 months, always giving you some certificates still valid before the validity is up.
- Note: Currently this is under discussion in the MCP forum

Meeting notes (2/2)

- There is now a SECOM Service Specification and SECOM Service Design Template registered in Navelink Service Registry that you can use. There is also a lot of work being done regarding the SECOM development such as the SECOM Hotel.
  - There are also an issue list for SECOM and if you want to see that list and the ongoing mitigations and discussions you can contact Navelink (info@navelink.org).
- A presentation and demo was given on S-125/S-201 e-Navigation services by Nikolaos Vastardis (R&D GLA UK & Ireland) (See slides 11-22)
  - Pact is a tool that is used to run quick test on service clients and how they expect the service to behave e.g. what we expect to receive in return when we send a specific request
  - The services exists on their GitHub, which are currently private, but there are plans to make them public in the next few days.
  - https://rnavlab.gla-rad.org
    - *Username: guest*
    - *Password: letmeingrad*
- Next meeting 2024-02-22

NAVELINK

Navelink.org