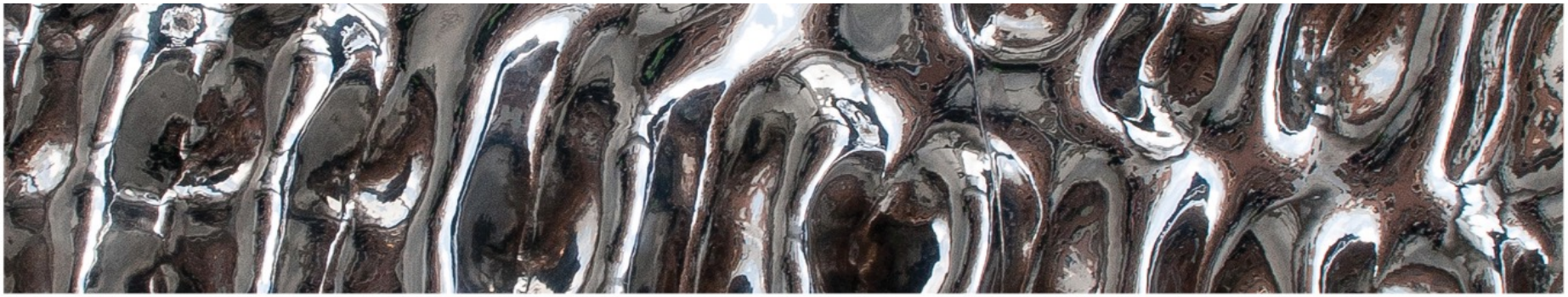


UiO : Department of Informatics
University of Oslo

# MCP III
# Brief introduction on MMS (Maritime Message Service) and MTS (Maritime Trust System)


Michael Kirkedal Thomsen

Associate Professor, Univ. of Copenhagen / Univ. of Oslo
Leader of MCC working group on Identities and security (IDSec)
m.kirkedal@di.ku.dk, michakt@ifi.uio.no


Technical seminar on SECOM and MCP, Oct 8-9 2025

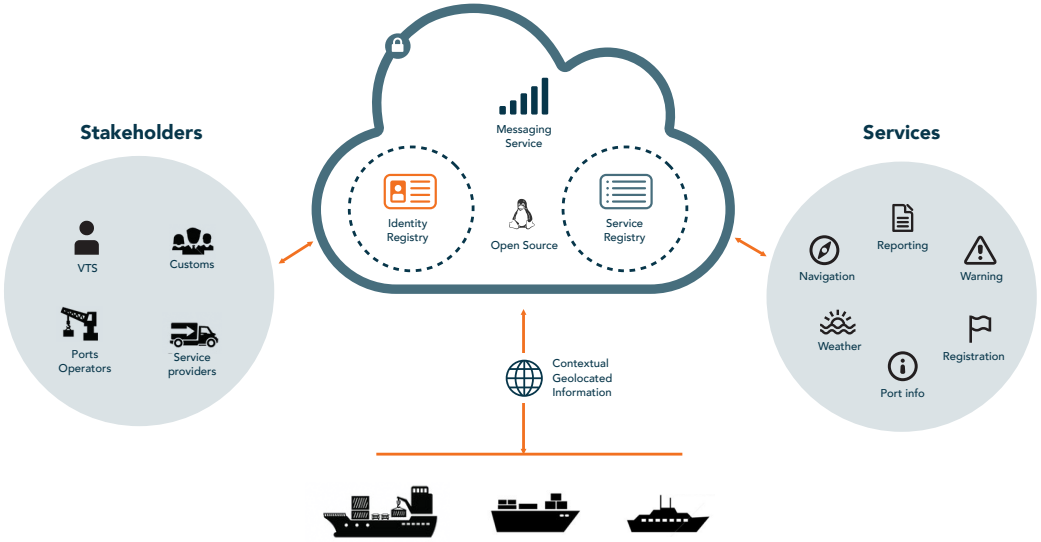
UNIVERSITY OF COPENHAGEN

UiO : Department of Informatics
University of Oslo

MCP

UNIVERSITY OF COPENHAGEN

# Maritime Connectivity Platform




Maritime Identity Registry

- Common and trusted identity understanding
- Commen scheme for identifyers (MRN)
- Harmonised API and definition of certificates in decentral architecture

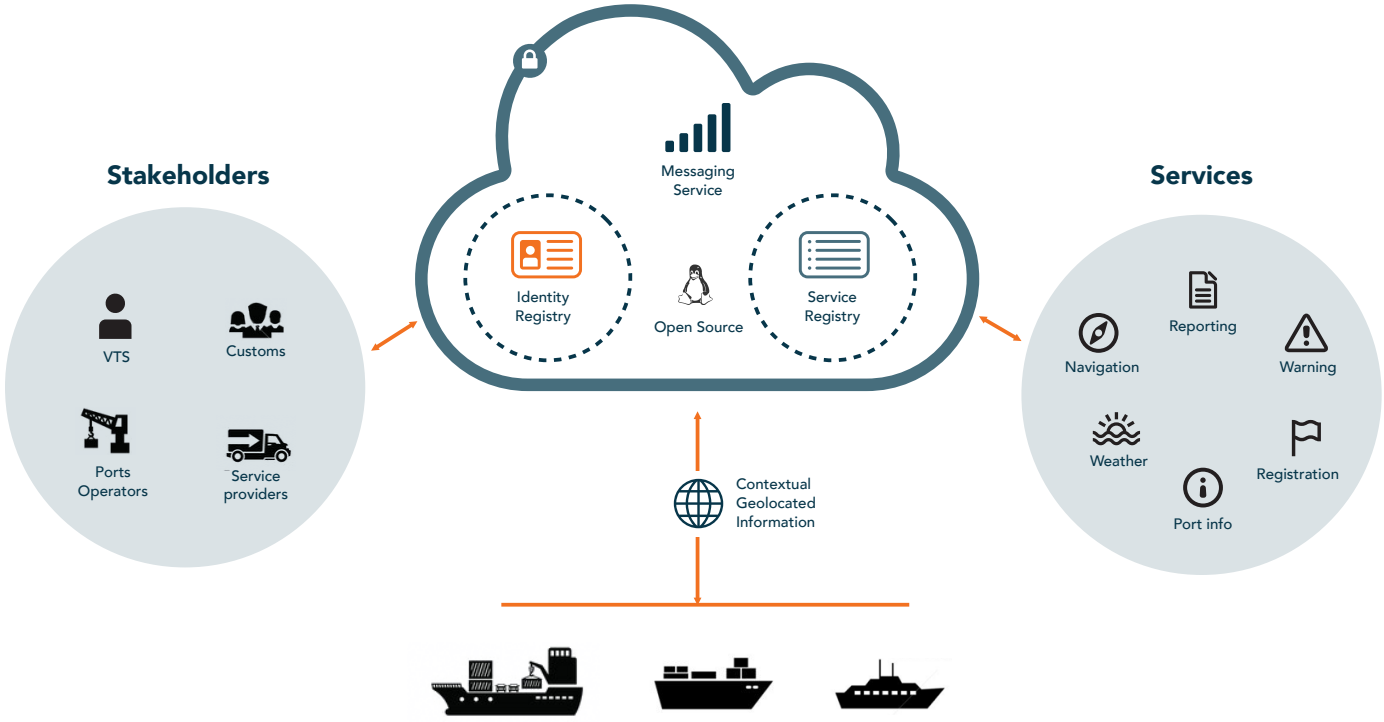
Maritime Service Registry

- Harmonised search and idenfitication of services

# MCP – What can we use identities for?

- Validate known identites (MRN/certificate)
- Ensure that all identies are different

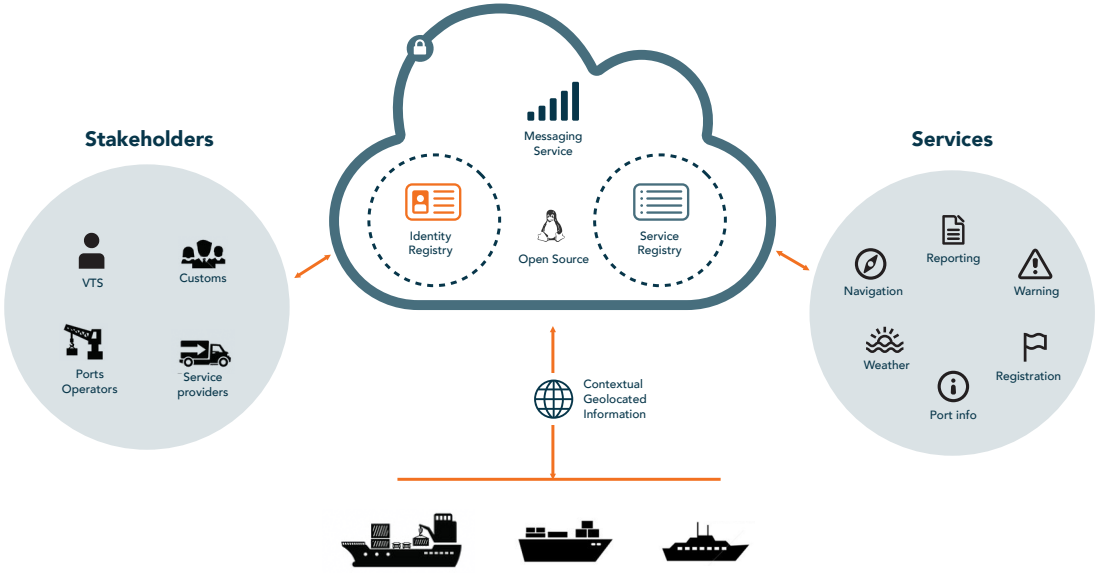
- The backbone of Internet security



# MCP – What does identites not give?

- Communication: Confidentiality, Integrity and Availability
- Relationships
  - Just because you know someone, you don't know their family tree.

- MRN has been used for this




- MRNs are tokens
- MRNs should not contain semantical information

# Applications of trusted identies

**All your services and applications**

- S-100 products
- …

**Communication Protocols**

SECOM

- Connection-based secure and authenticated communication

Maritime Message Service

- Message-based secure and authenticated communication
  - with subscription functionality

**Authorisation and Relation Handling**

Maritime Trust System

- Decentral and Trusted relations
- (ongoing work)

UiO : Department of Informatics
University of Oslo

MCP

UNIVERSITY OF COPENHAGEN

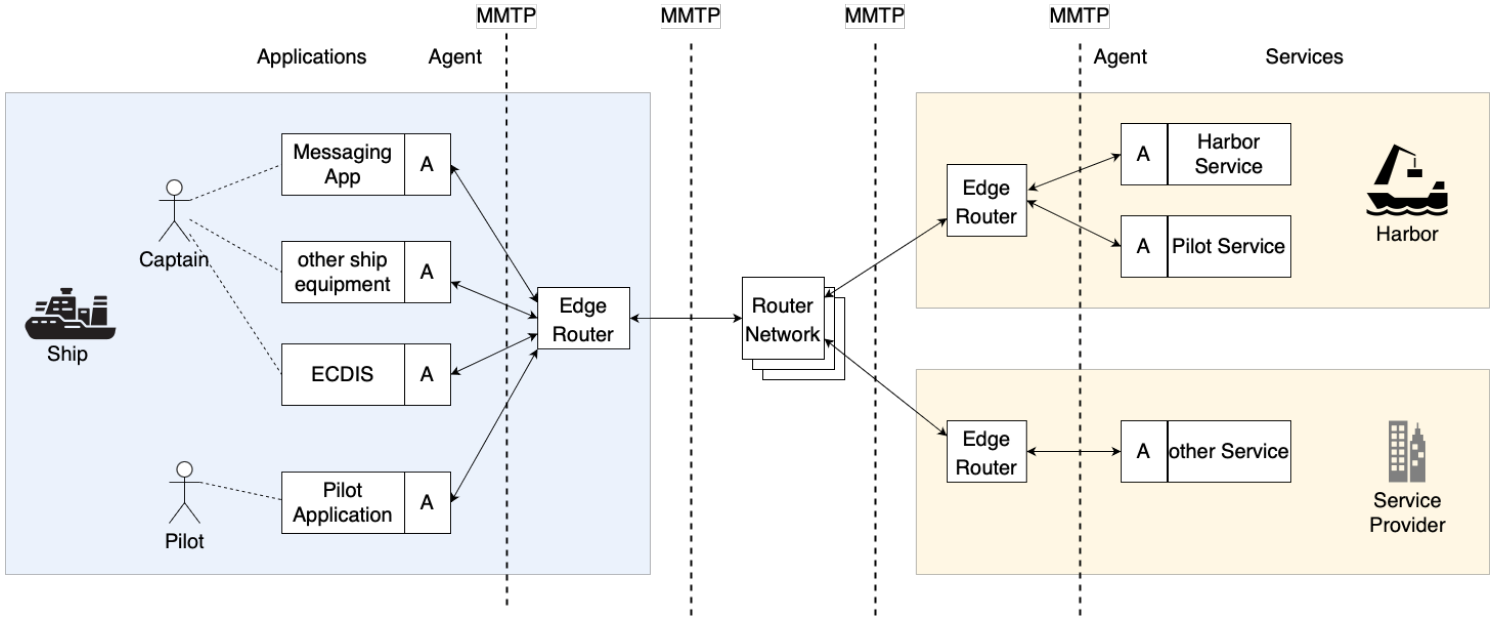
# MCP – Maritime Messaging Service


- Secure and reliable store-and-forward messages
- Distribution of data based on known identities (MCP certificated)
- Topic-cast authenticated messages based on subscriptions

# MMS – Maritime Messaging Service

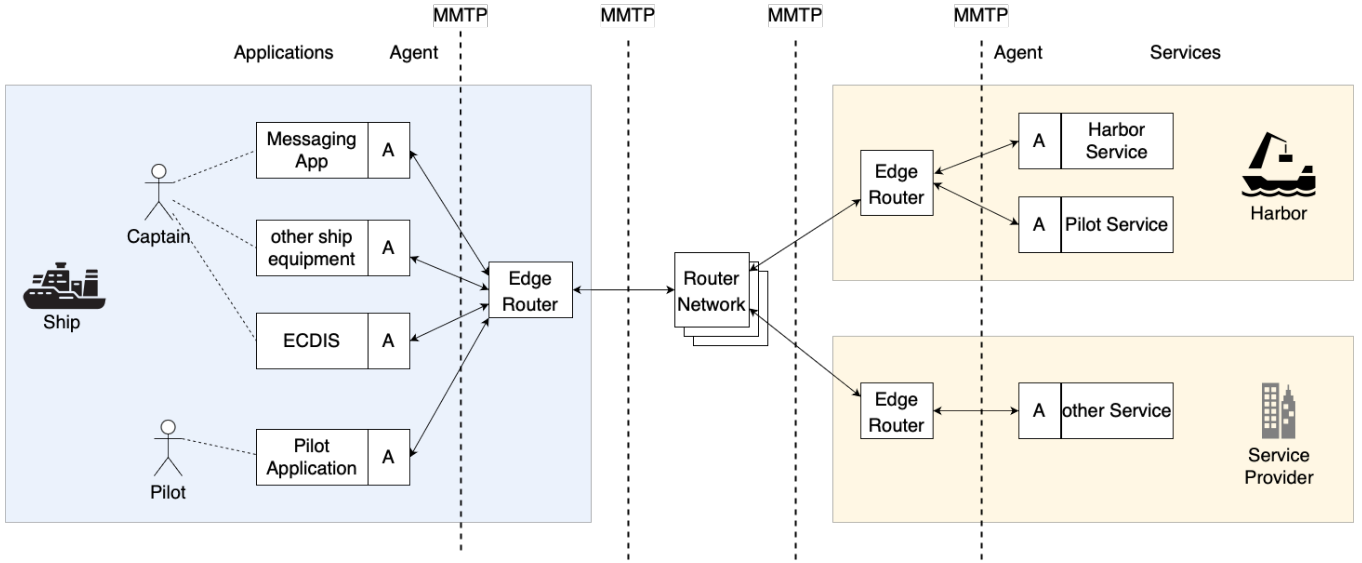
- Secure and reliable store-and-forward messages
- Distribution of data based on known identities (MCP certificated)
- Topic-cast authenticated messages based on subscriptions

- MMS is standardised in ”**RTCM Standard 13900.0, Maritime Messaging Service Architecture and Protocol**”
  - https://maritimeconnectivity.net/mcp-documents/#MMS



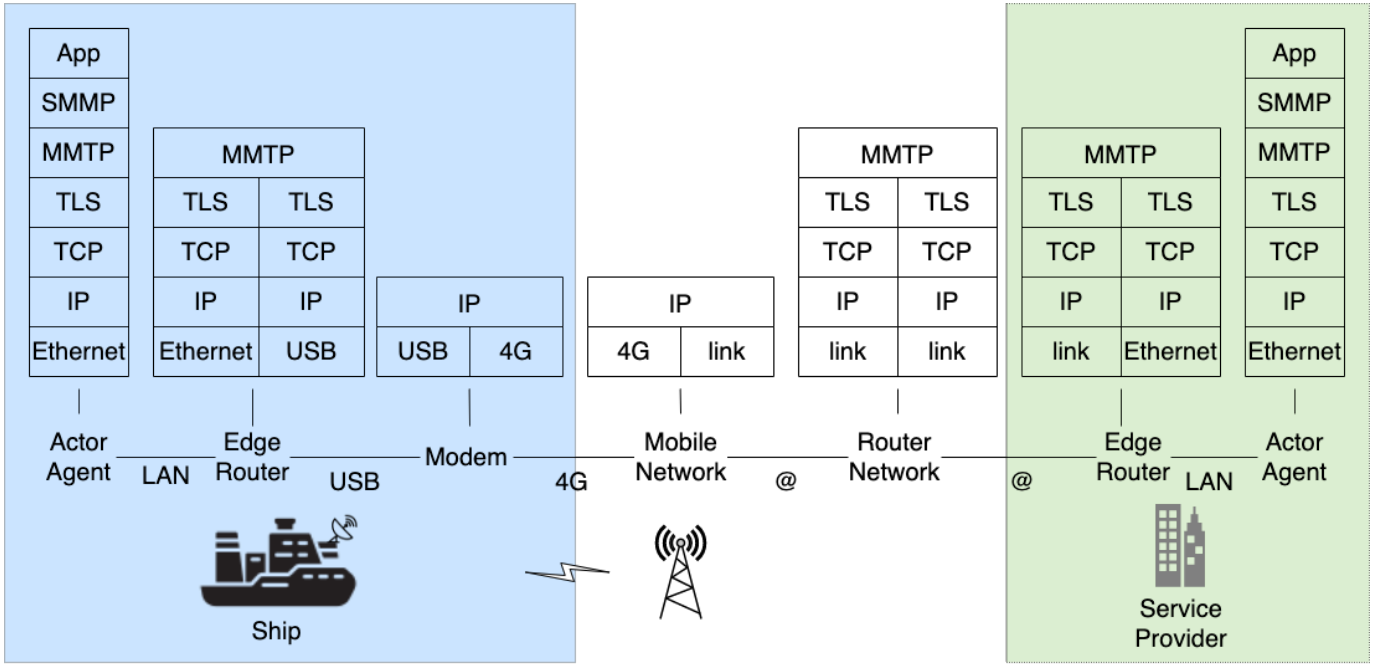
# MMS – Architecture (3 layers)

- MMS Agents
  - Local application interface or client
  - The layer to which service and application will connect
- MMS EdgeRouters
  - Outer message parsing interface
  - Highly ”configurable”, suitable for different transport and local applicatons
- MMS RouterNetwork
  - Backbone handling of message parsing – most will never know about this



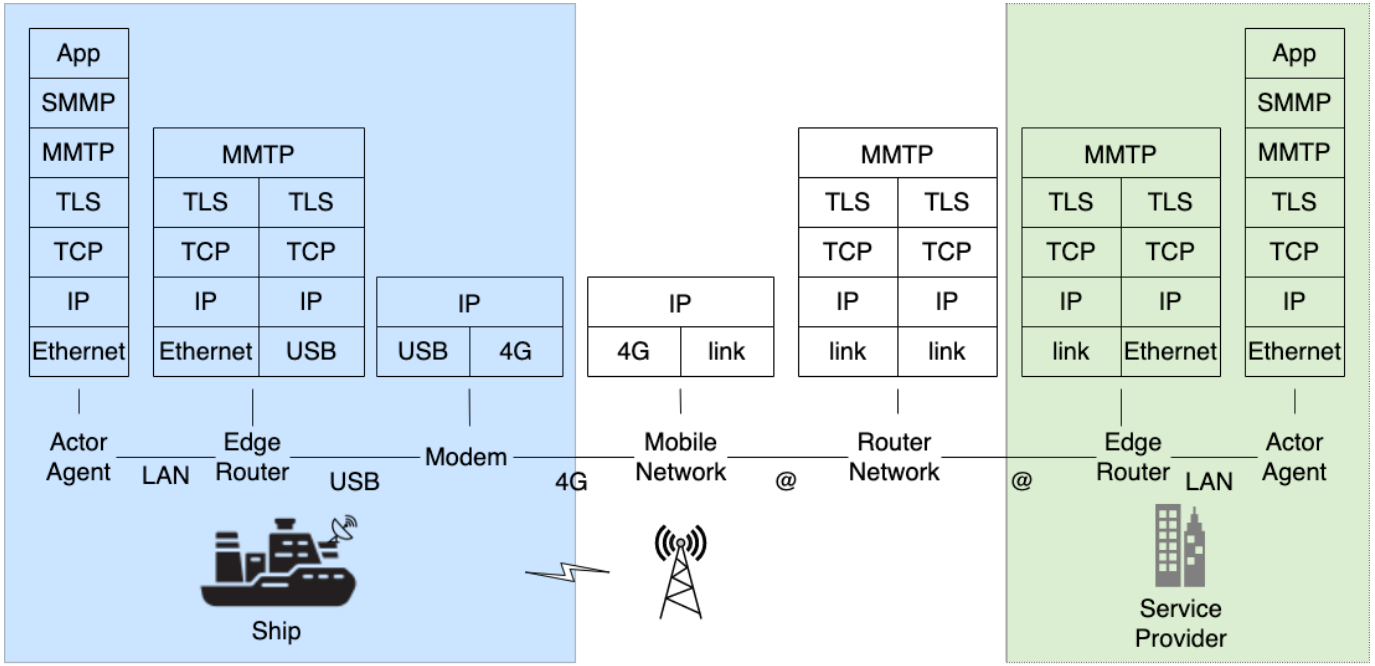
# MMS – Protocols (3 layers)

- SMMP: Secure Maritime Message Protocol
  - End-to-end message guarentees
  - Confidentiality, delivery guarantee, non-repudiation, message segmentation
- MMTP: Maritime Message Transfer Protocol
  - Message routing, agent subscriptions, topic-cast and direct messages
  - Includes message autentication
- Transport Protocol
  - TCP/IP, VDES, etc.



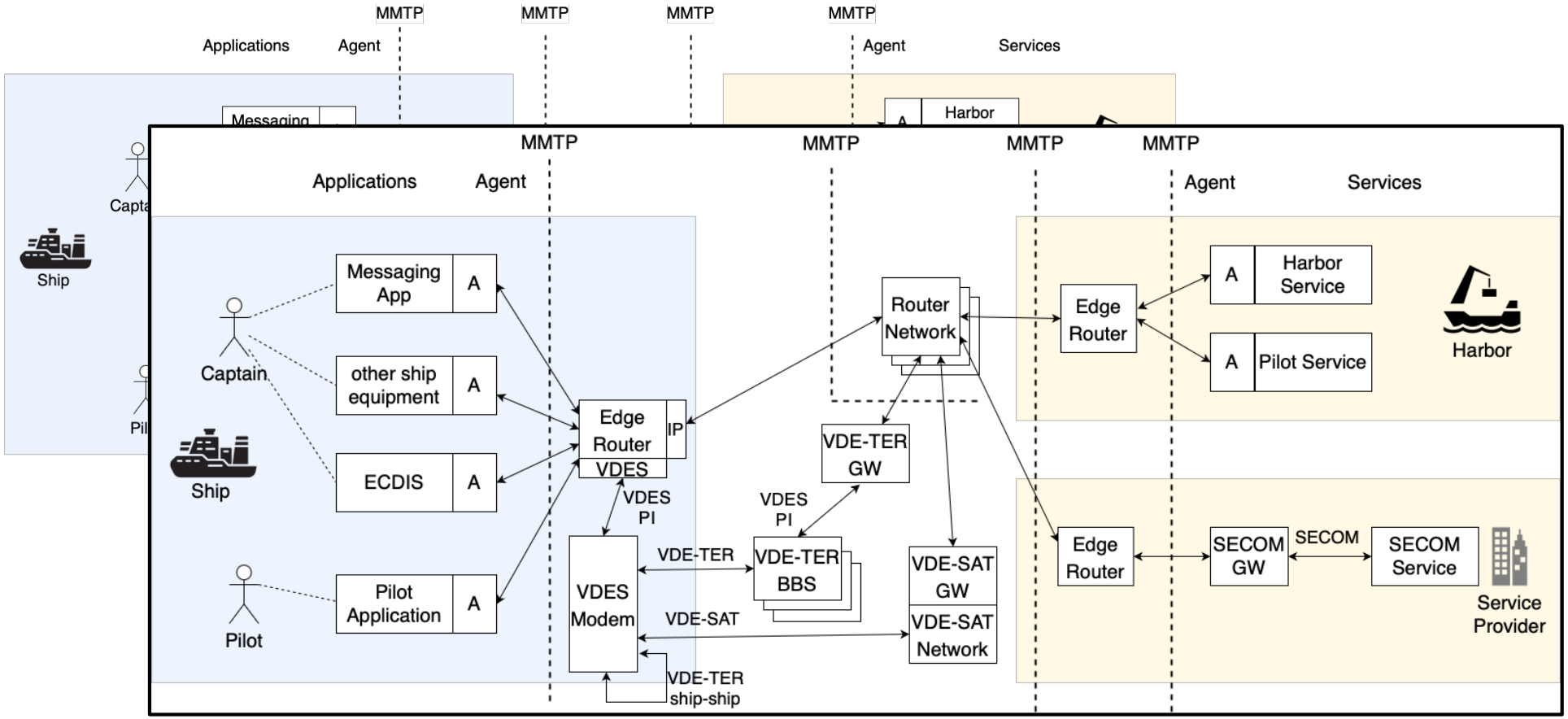
# MMS – Protocols (3 layers)

- SMMP: Secure Maritime Message Protocol
  - End-to-end message guarentees
  - Confidentiality, delivery guarantee, non-repudiation, message segmentation
- MMTP: Maritime Message Transfer Protocol
  - Message routing, agent subscriptions, topic-cast and direct messages
  - Includes message autentication
- Transport Protocol
  - TCP/IP, VDES, etc.



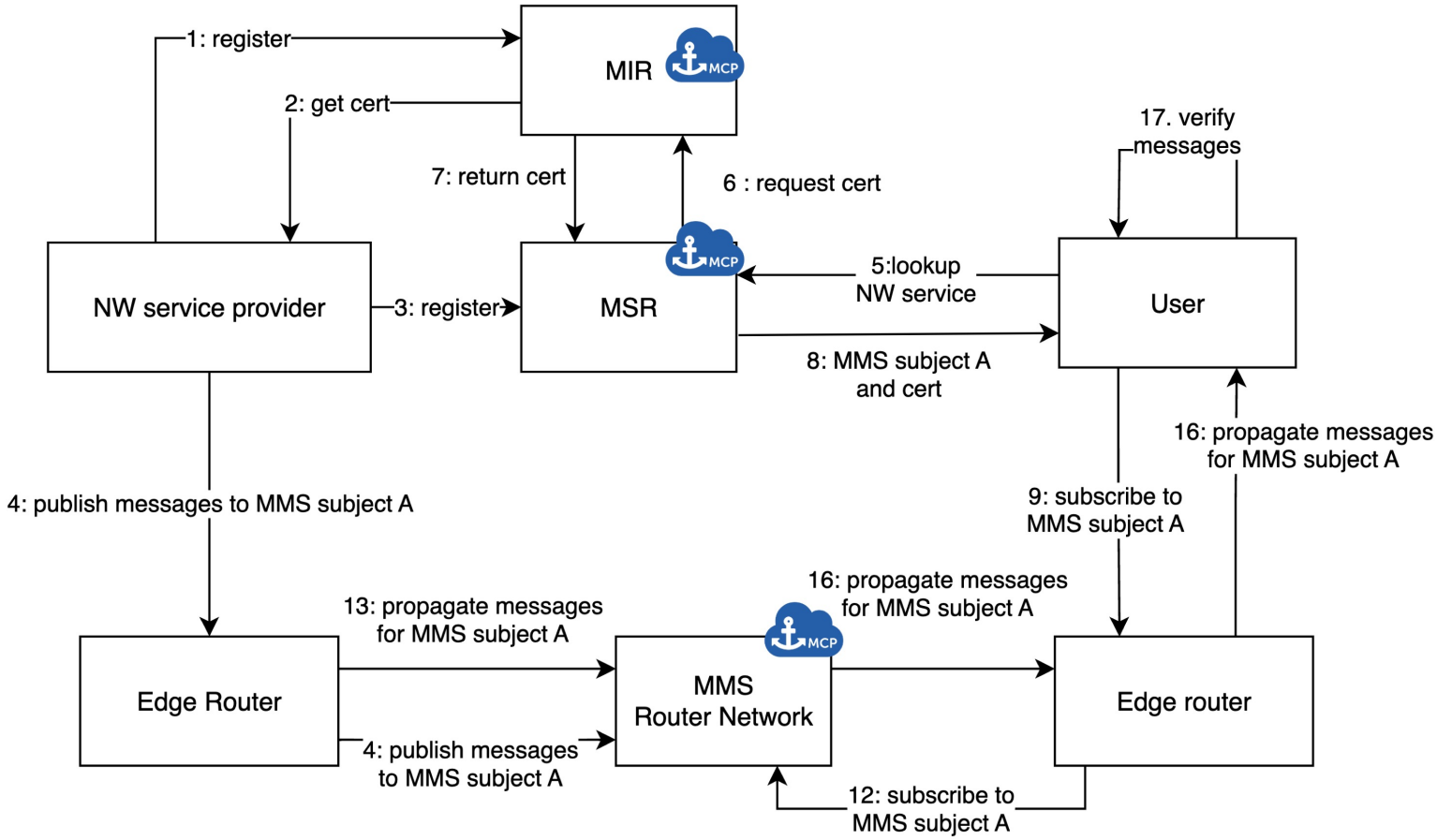
# MMS – Transport agnostic

- MMS is designed to be transport agnostic.
  - TCP/IP (with TLS on individual connections), VDES (TER + SAT), etc.
- Transport methods are handled between EdgeRouter and RouterNetwork



# MMS – Integration and message distribution

- MMS integaration with MIR and MSR
- Subscriptions to topics

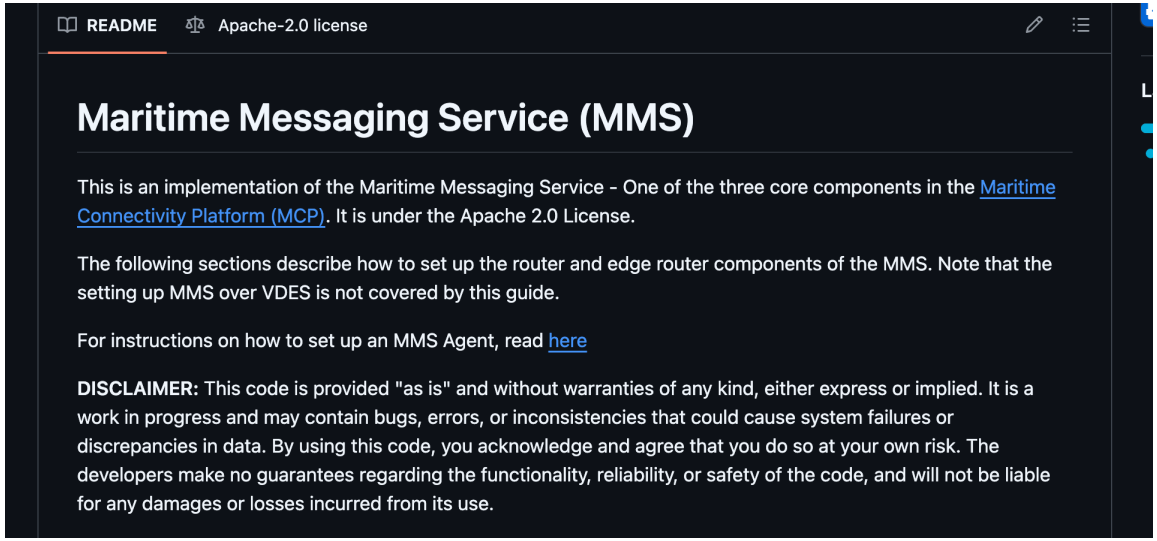


UiO : Department of Informatics
University of Oslo

UNIVERSITY OF COPENHAGEN

# MMS – Implementation

- Open source implementation af router og edge router
  - https://github.com/maritimeconnectivity/MMS
- Browser-based MMS agent
  - https://github.com/Team-AIVN/mms-browser-agent
- MMS is standardised in ”**RTCM Standard 13900.0, Maritime Messaging Service Architecture and Protocol**”
  - https://maritimeconnectivity.net/mcp-documents/#MMS
  - https://www.vdes-alliance.org/index.php/2025/04/09/rtcm-publishes-mms-standard/



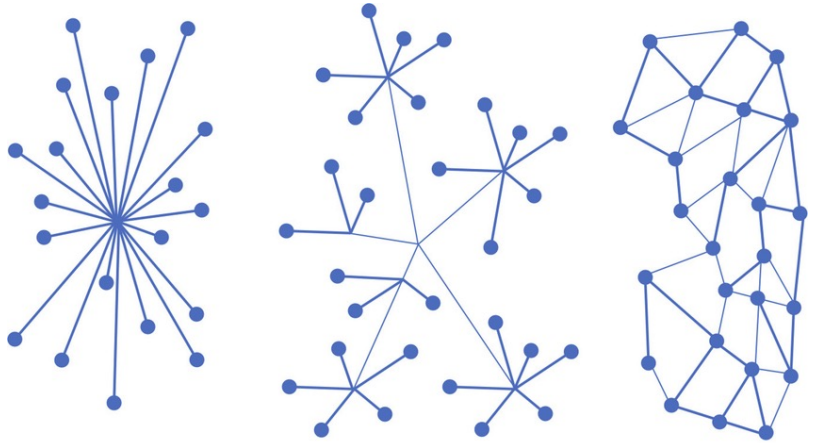

# MCP – Maritime Trust System

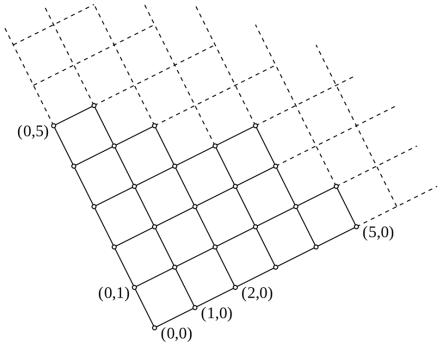
- Can be used to define complex relations between MCP identities
- Examples:
  - Know that an AtoN (certificate) belongs to a specific authority
  - Know an identity belongs to a habour, person, captain, etc.
  - Know that a service can procide data to an ECDIS
  - …

- The trust system will not define relationships
  - This will be done by IALA guidelines and similar
- Trust anchors are to be defined by relevant organisations
-

# MTS - design

- De-central handling of delegations
  - Delegating trust
  - Authorizing trust
  - Communication agnostic
  - Off-line validation
- Trust delegations are:
  - Cryptographic proofs (signatures)
  - Founded in MCP (X.509) certificates
- Trust relations will be defined by
  - a restricted domain-specific trust programming language




```
language <capability>, <authority>, <area> {
    <capability> :: tdns(atomic)
    <authority>  :: tdns(atomic)
    <area>       :: tdns(atomic)
}

local group vessel          = [vessel1, vessel2]
local group authority_pilot = [NCA]
policy pilotAuthNO = authority:{pilot},area:{norway}

trust all(vessel) -> all(authority_pilot)
  = pilotAuthNO
restricted trust all(authority_pilot) -> pilot1
  = capability:{pilot},area:{norway.bergen}
  ; capability:{pilot},area:{norway.stavanger}
restricted trust all(authority_pilot) -> pilot2
  = capability:{pilot},area:{norway.oslo}

trust pilot1 -> pilot2
  = capability:{pilot},area:{norway.bergen}
  ; capability:{pilot},area:{norway.stavanger}
```

UiO : Department of Informatics
University of Oslo

MCP

UNIVERSITY OF COPENHAGEN

# Maritime Trust System

- Working towards a first draft IALA Guideline for MTS to DTEC6, Spring 2026.
- We invite everyone to join the work in the MCC IDSec working group
  - Contact me, Juho or Thomas

# Questions?

**Maritime Message Service**

- Message-based secure and authenticated communication
  - with subscription functionality

**Maritime Trust System**

- Decentral and Trusted relations
- Authorisation and Relation Handling