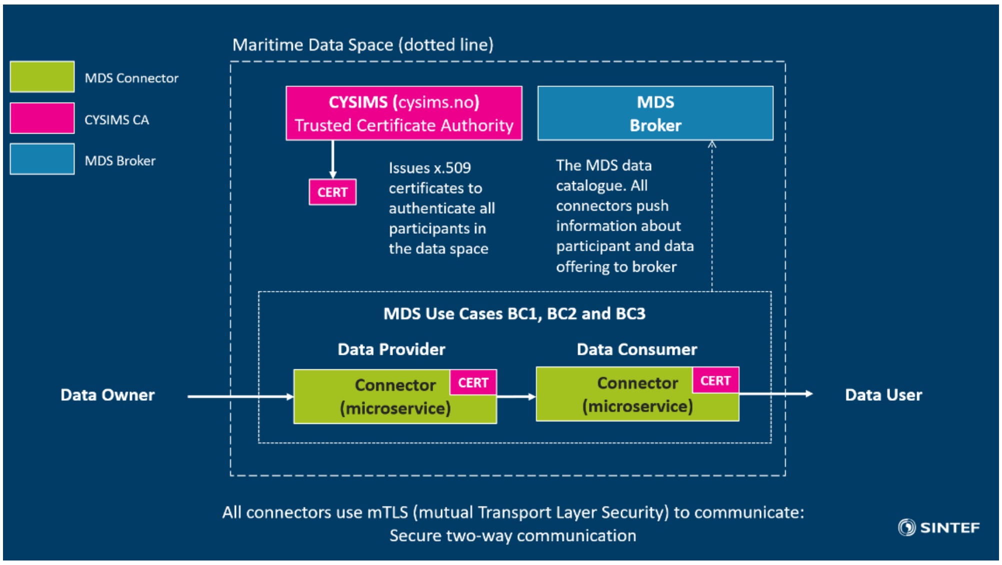
MDS-D1.4- Unrestricted

Maritime Data Space (MDS)

Final Project Report

D1.4 Maritime Data Space platform - including data models and communication

Authors
Bjørn Marius von Zernichow
Dag Atle Nesheim


Maritime Data Space (dotted line)
MDS Connector
CYSIMS CA
MDS Broker
CYSIMS (cysims.no)
Trusted Certificate Authority
CERT
Issues x.509 certificates to authenticate all participants in the data space
MDS
Broker
The MDS data catalogue. All connectors push information about participant and data offering to broker
MDS Use Cases BC1, BC2 and BC3
Data Provider
Data Consumer
Data Owner
Connector (microservice)
CERT
Connector (microservice)
CERT
Data User
All connectors use mTLS (mutual Transport Layer Security) to communicate: Secure two-way communication
SINTEF

SINTEF Digital
SD-Smart Data
2021-06-30

SINTEF Digital
SINTEF Digital

Address:
Postboks 124 Blindern
NO-0314 Oslo
NORWAY
Switchboard: +47 40005100

info@sintef.no

Enterprise /VAT No:
NO 919 303 808 MVA

End User Documentation

Final Project Report

D1.4 Maritime Data Space platform - including data models and communication

KEYWORDS:
MDS, IDSA, data sharing, maritime

VERSION 1.0	**DATE** 2021-06-30

AUTHOR(S)
Bjørn Marius von Zernichow
Dag Atle Nesheim

CLIENT(S) NAVTOR	**CLIENT'S REF.** NAVTOR
PROJECT NO. 102019389	**NUMBER OF PAGES:** 29

ABSTRACT

Maritime Data Space (MDS)

The innovation project Maritime Data Space (MDS) has developed a federated ecosystem for secure, efficient, and trusted exchange and sharing of ship related data among trusted stakeholders on ship and shore. The core technology and business aspects of MDS is based on the reference architecture and guidelines promoted by the International Data Spaces Association (IDSA).

The innovation of the project has been validated in 3 business cases, and we have demonstrated that MDS: 1) Provides transparent access to ship related data from anywhere on ship or shore, 2) Enables secure, robust, and efficient communication between ship and shore, and 3) Digitalizes and simplifies the provision of trusted services for day to day operation of the ship.

PREPARED BY Bjørn Marius von Zernichow	SIGNATURE BMZernichow
CHECKED BY Till C. Lech	SIGNATURE Till C Lech
APPROVED BY Dag Atle Nesheim	SIGNATURE Dag Atle Nesheim

REPORT NO.	ISBN	CLASSIFICATION	CLASSIFICATION THIS PAGE
MDS-D1.4	ISBN	Unrestricted	Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
1.0	2021-06-30	Final project report and end user documentation

Table of contents

1 Introduction

The innovation project Maritime Data Space (MDS) has developed a federated ecosystem for secure, efficient, and trusted exchange and sharing of ship related data among trusted stakeholders on ship and shore. The core technology and business aspects of MDS is based on the reference architecture and guidelines promoted by the International Data Spaces Association (IDSA).

The innovation of the project has been validated in 3 business cases, and we have demonstrated that MDS:

1. **Provides transparent access to ship related data** from ship or shore
2. **Enables secure, robust, and efficient communication** between ship and shore
3. Digitalizes and **simplifies the provision of trusted services** for day-to-day operation of the ship

More and more digital ship data is produced on board the ship, from increased digitalization and cheaper sensor technology, but also from yards, ship equipment vendors, interest organizations, class societies and authorities. To make use of this data, service providers want to offer new functionalities related to data analysis, customer empowerment, automated reporting, process improvement and quality monitoring. Today, data sharing with service providers is done on an ad hoc basis where the data access agreements must be negotiated case-by-case and often involving several different parties. In the MDS project, we have developed an open framework where the deployment of services, management and governance of data and creation of digital contracts are user driven, and not linked to specific information providers.

1.1 Transparent access to ship related data

Since data is often produced and owned by other parties than those providing services based on the data, there was a need for a new model for trusted sharing of data. We required a model where the data owners directly control access rights, independently of where the data is stored. In the maritime sector, no such standard mechanisms exist. In this project, we have adapted the data sharing and exchange mechanisms defined within the Industrie 4.0 related IDSA approach. IDSA focuses on trusted data exchange and sharing, with support for strong data sovereignty and control for data owners. It uses modern cryptographic methods to maintain records of ownership of data objects, independently of where the objects are stored. The data owner, which is identified by its electronic signature, can then provide secure access to third party data consumers. Principles from IDSA have been combined with the current developments in maritime communication technology and data management platforms from Veracity by DNV, and the result is a new data and service integration concept for modern shipping.

1.2 Secure and efficient communication between ship and shore

User authentication and authorization, secure data transfer and proof of data ownership (trusted identity) have been implemented, supported by the IDSA Reference Architecture. Data providers and consumers use mTLS (mutual Transport Layer Security) to communicate securely in all business cases based on two-way authentication with CySIMS certificates. All actors will prove their identity to the Maritime Data Space using a certificate issued by the CySIMS Certificate Authority. Authorization of user access to data offerings is enabled by use of the unique thumbprint of each certificate to allow and restrict access. In addition, all MDS participants are assigned a custom domain. Each certificate is again linked to this unique domain, and this forms the basis of the MDS ecosystem.

1.3 Simplified provision of trusted services

The project has demonstrated the benefits of the IDSA framework by implementing 3 pilot cases selected by the industry partners as being representative for the next generation of digital ship services. This shows the easy and secure realisation of these new maritime services with focus on distributed management and governance of ship related data using secure peer-to-peer communication between value chain actors. MDS defines a new and open digital ecosystem for the maritime community where data can be made efficiently and securely available and where new and improved services can be developed and deployed on a distributed platform. Furthermore, the Veracity by DNV data and service platform has been used to support the main business case of MDS – EU MRV Reporting – to collect and analyse shipping emissions data that is needed for mandatory environmental performance management in maritime shipping.

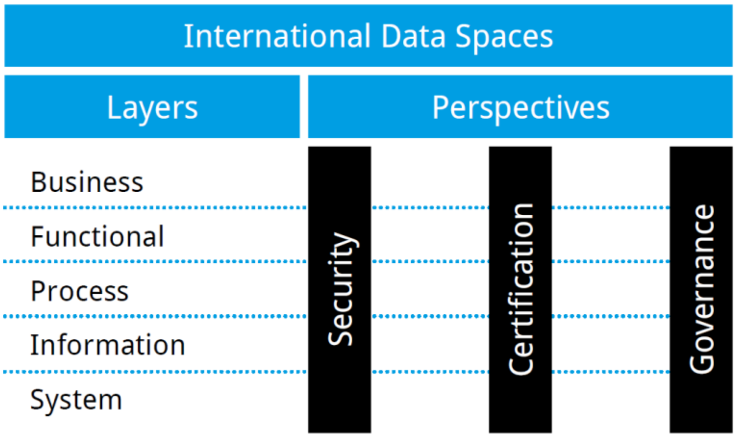
2 The IDSA Reference Architecture Model as a blueprint for the MDS Ecosystem

In compliance with common system architecture models and standards (e.g., ISO 42010, 4+1 view model), the IDSA Reference Architecture Model uses a five-layer structure expressing various stakeholders' concerns and viewpoints at different levels of granularity. In this context, the concept of **Data Spaces** can be defined as ecosystems for secure and trusted data exchange based on the principles and Reference Architecture Model promoted by IDSA. Furthermore, *MDS will be defined as an implementation of such a Data Space*. The general structure of the Reference Architecture Model is illustrated in

Figure 1 - General structure of the IDSA Reference Architecture Model. The model consists of five layers:

- The **Business Layer** specifies the different roles which the participants of the Data Space can assume, and it specifies the main activities and interactions related to each of these roles.
- The **Functional Layer** defines the functional requirements of the Data Space, including the specific features to be derived from these.
- The **Process Layer** specifies the interactions taking place between the different components of the Data Space by using the BPMN notation.
- The **Information Layer** defines a conceptual model which makes use of linked-data principles to describe both the static and the dynamic aspects of the participants, technological components, and data offerings.
- The **System Layer** describes implementation of technological components – such as integration, configuration, deployment, and extensibility of software components.

In addition to the five dimensions listed above, the Reference Architecture Model comprises three perspectives that need to be implemented across all five layers: *Security, Certification, and Governance.*



The final documentation of MDS in this project report, will be structured around the five dimensions of the IDSA Reference Architecture Model – and include the cross-cutting perspectives on Security, Certification and Governance.

Figure 1 - General structure of the IDSA Reference Architecture Model

2.1 The MDS Business Layer

The **Business Layer** specifies the different roles which the participants of the Data Space can assume, and it specifies the main activities and interactions related to each of these roles. In this sense, the Business Layer contributes to the development of innovative business models and digital, data-driven services to be used by the participants in a Data Space. The Business Layer provides an abstract description of the roles in a Data Space, and can be considered a blueprint for the other, more technical layers. Hence, the Business Layer specifies the requirements to be addressed by the Functional Layer. There are four categories of roles: 1) Core Participants, 2) Intermediaries, 3) Software and Service Providers, and 4) Governance Body.

2.1.1 Core Participant Roles

Core Participants are involved and required every time data is exchanged in the Data Space. Roles assigned to this category are *Data Owner, Data Provider, Data Consumer,* and *Data User.* The role of a Core Participant can be assumed by any organization that owns, wants to provide, and/ or wants to consume or use data.

- A **Data Owner** can be defined as a legal entity or natural person that produces data and/ or executes control over it. The Data Owner will define Data Usage Policies and provides access to data.
- Usually, a participant acting as Data Owner automatically assumes the role of the **Data Provider** as well. The Data Provider makes data available for exchange between a Data Owner and a Data Consumer. Furthermore, the Data Provider will communicate information about the Data Owner and their data offerings to a centralized *Broker Service Provider* that holds and displays metadata collected from all available Data Providers in the Data Space.
- The **Data Consumer** receives data from a Data Provider. From a business process modelling perspective, the Data Consumer is the mirror entity of the Data Provider; the activities performed by the Data Consumer are therefore similar to the activities performed by the Data Provider. A Data Consumer can search for and query available data offerings by interacting with the user interface of the Broker Service Provider. A Data Consumer can either connect to a Data Provider directly or via the Broker Service Provider.
- The **Data User** is the legal entity that has the legal right to use the data of a Data Owner as specified by the usage policy. This role is similar to the Data Owner being the legal entity that has the legal control over its data. In most cases, the Data User is identical to the Data Consumer.

2.1.2 Intermediary Roles

Intermediaries act as trusted entities in the Data Space that establish trust and provide metadata and data catalogue functionality. In this sense, the Intermediary Roles create a business model environment around data and services being offered. The Intermediary Roles include 1) The Identity Provider, 2) The Broker Service Provider, and 3) The Clearing House.

- The **Identity Provider** offers a service to create, maintain, manage, monitor, and validate identity information of participants in the Data Space. The Identity Provider consists of a **Certificate Authority** that manages digital certificates and a Dynamic Attribute Provisioning Service that manages dynamic attributes such as authorized access to data offerings.
- The **Broker Service Provider** is a centralized role that stores and manages information about participants and data offerings. The activities of the Broker Service Provider mainly focus on receiving and providing metadata which must be described according to the IDSA Information Model. It is important to notice that the Broker Service Provider is not involved in the data exchange. After the Broker Service Provider has provided the Data Consumer with the metadata

about a certain Data Provider, its job is done, and it is not involved in the subsequent data exchange process.

- The **Clearing House** is an intermediary that provides clearing and settlement services for all financial and data exchange transactions. The clearing activities are separated from broker services since these activities are technically different from maintaining a metadata repository. The Clearing House logs all activities performed during a data exchange. After a data exchange, or parts of it, has been completed, both the Data Provider and the Data Consumer confirm the data transfer by logging the details of the transaction at the Clearing House. Based on this logging information, the transaction can then be billed, and the logging information can also be used to resolve conflicts.

2.1.3 Software and Service Provider Roles

These roles provide software and services to be used by the participants in the Data Space. The Service Provider can host the required infrastructure for participation in the Data Space in case a participant does not deploy the needed technical infrastructure itself. The Service Provider role also includes the provision of additional data services (e.g., for data analysis, data integration, data cleansing, or semantic enrichment) to improve the quality and usefulness of the data exchanged in the ecosystem.

2.1.4 Governance Body Roles

The Certification Body, Evaluation Facilities, and the International Data Spaces Association (IDSA) are the Governance Bodies of the Data Space.

- The Certification Body and the Evaluation Facilities certify the participants and the core technical components in the Data Space. The Governance Bodies ensure that only certified and compliant organizations are granted access to the trusted business ecosystem. The Certification Body supervises the activities, actions, and decisions of an Evaluation Facility.
- IDSA is a non-profit organization that supports and governs the development of the Reference Architecture Model and the participant certification process.

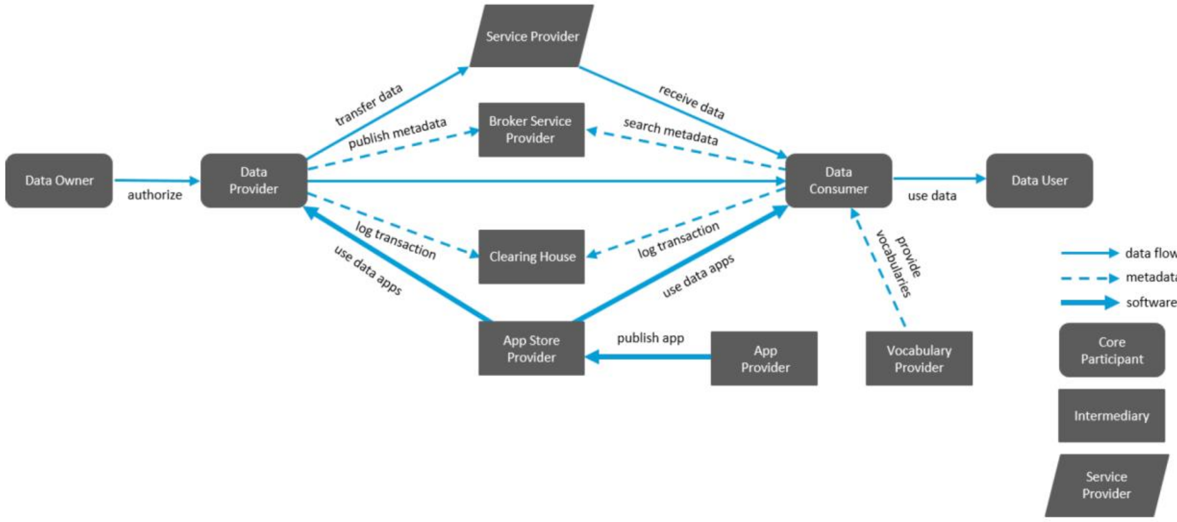


Figure 2 - Roles and interactions as defined by the IDSA Reference Architecture Model

3 Access to source code and implementation of the IDSA Roles in MDS

The source code for implementation of IDSA Roles in the MDS project is available for project partners at the following GitHub repositories:

- https://github.com/maritime-data-space (private repository)
- https://github.com/maritime-data-space/cysims-certificate-authority (private repository)
- https://github.com/maritime-data-space/connectors-broker (private repository)
- https://github.com/veracity/MDSConnector (public repository)

The table below describes how the specific IDSA roles outlined in Figure 2 and sections 2.1.1 to 2.1.4 have been implemented in the MDS ecosystem. Each actor can assume several roles.

Role	MDS Participants					
	NAVTOR	NEURON SOLUTION	DNV	WILHELMSEN	IMO DSC/ EU MRV	CYSIMS
Data Owner	BC2			BC1, BC3		
Data Provider	BC2	BC1, BC3				
Data Consumer	BC3		BC1	BC2		
Data User	BC3			BC2	BC1	
Identity Provider						BC1, BC2, BC3
Service Provider		BC1, BC3	BC1			
Broker Service	Operated by SINTEF Digital within the context and duration of the MDS project					
Clearing House	Outside of scope of the MDS project					
Certification Body	Outside of scope of the MDS project					

BC1 = Business Case 1, BC2 = Business Case 2, BC3 = Business Case 3

The MDS project has validated and demonstrated the IDSA approach for data sharing in three different business cases related to the maritime domain:

- Business Case 1 – EU MRV Reporting
- Business Case 2 – Vessel Speed/ ETA Management
- Business Case 3 – Ship Reporting

4 The MDS Business Cases

The MDS ecosystem for data sharing is based on the reference architecture of the International Data Spaces Association (IDSA), and includes the following main components and actors as illustrated by Figure 3 below:

- The **Connectors** – here illustrated as green boxes – are responsible for the exchange of data as it executes the complete data sharing process from the internal data resources at Data Provider side to the Data Consumer side. The Connector provides metadata to a Broker about its technical interface description, and exposed data sources, along with associated data usage policies. It is important to note that the data is transferred directly between the Connectors of the Data Provider and the Data Consumer according to a decentralized peer-to-peer network concept. Hence, there is no centralized technical component in the Maritime Data Space that mediates data exchange between participants.
- The **Identity Provider** offers a service to create, manage, and validate identity information of participants in MDS. The Identity Provider consists of a **Certificate Authority (CYSIMS)** that

manages digital certificates. All connectors use mTLS (mutual Transport Layer Security) to communicate securely in all business cases based on two-way authentication with CYSIMS certificates. All connectors will prove their identity to the Maritime Data Space using a certificate issued by a CySIMS Certificate Authority. Authorization of user access to data offerings is enabled by use of the unique thumbprint of each certificate to allow and restrict access. In addition, all MDS participants are assigned a custom domain. Each certificate is again linked to this unique domain, and this forms the basis of the MDS ecosystem. As an example, the Navtor connector is assigned the custom domain https://mdsconnector01.tk.

- The **Broker Service Provider** is a centralized role that stores and manages information about participants and data offerings. The activities of the Broker Service Provider mainly focus on receiving and providing metadata which must be described according to the IDSA Information Model, but the Broker Service Provider is not involved in the actual data exchange. After the Broker Service Provider has provided the Data Consumer with the metadata about a certain Data Provider, its job is done, and it is not involved in the subsequent data exchange process.

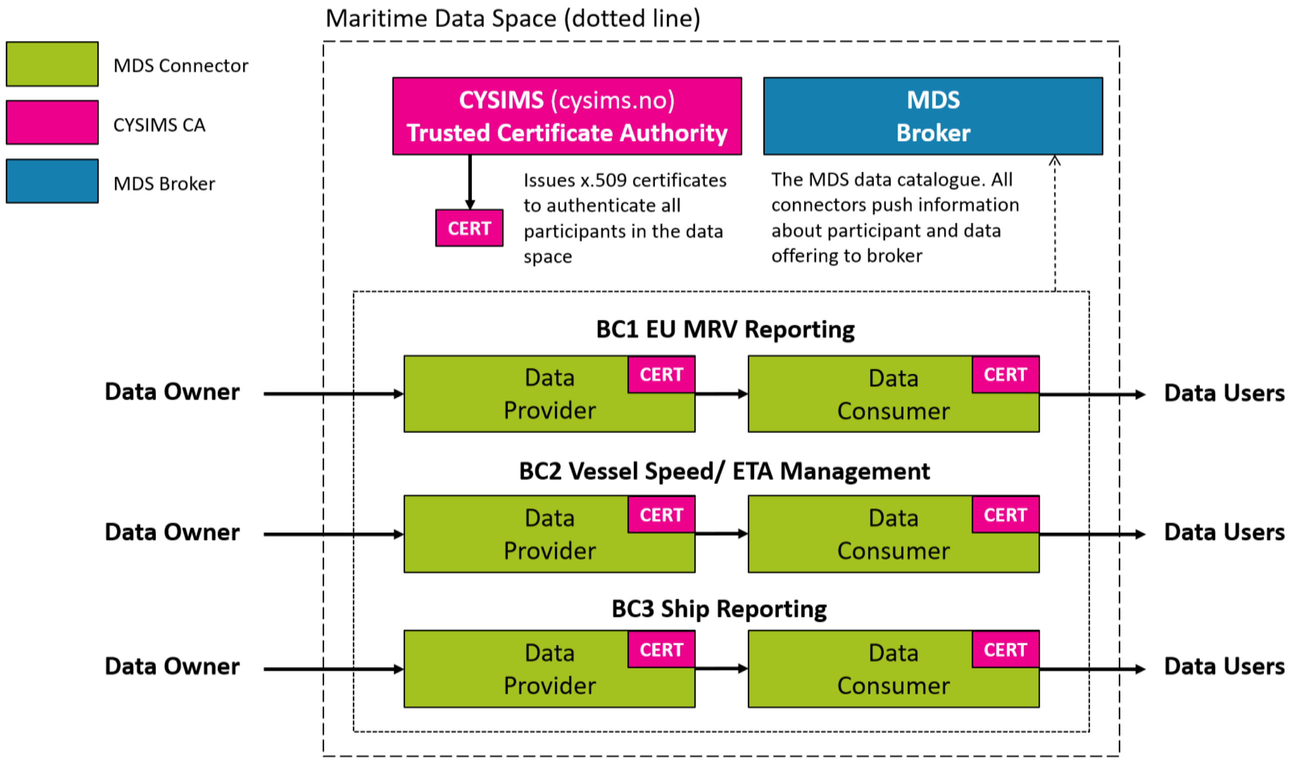

Maritime Data Space (dotted line)
MDS Connector
CYSIMS CA
MDS Broker
CYSIMS (cysims.no)
Trusted Certificate Authority
MDS
Broker
CERT
Issues x.509 certificates to authenticate all participants in the data space
The MDS data catalogue. All connectors push information about participant and data offering to broker
BC1 EU MRV Reporting
Data Owner
Data Provider
CERT
Data Consumer
CERT
Data Users
BC2 Vessel Speed/ ETA Management
Data Owner
Data Provider
CERT
Data Consumer
CERT
Data Users
BC3 Ship Reporting
Data Owner
Data Provider
CERT
Data Consumer
CERT
Data Users

Figure 3 - General technical setup for all MDS business cases

4.1 Business Case 1 – Automatic EU MRV Reporting

The EU MRV business case is all about reporting efficiency. The Maritime Reporting and Verification regime, or MRV in short, is a regulatory requirement for all ships sailing to, from or between European ports. Through a Recognized Organization, the shipping company is obliged to send information regarding emissions per voyage, to EMSA. Currently this is a cumbersome process, involving manual reporting and processing of data. Figure 4 shows the manual reporting process prior to the start of the MDS project.

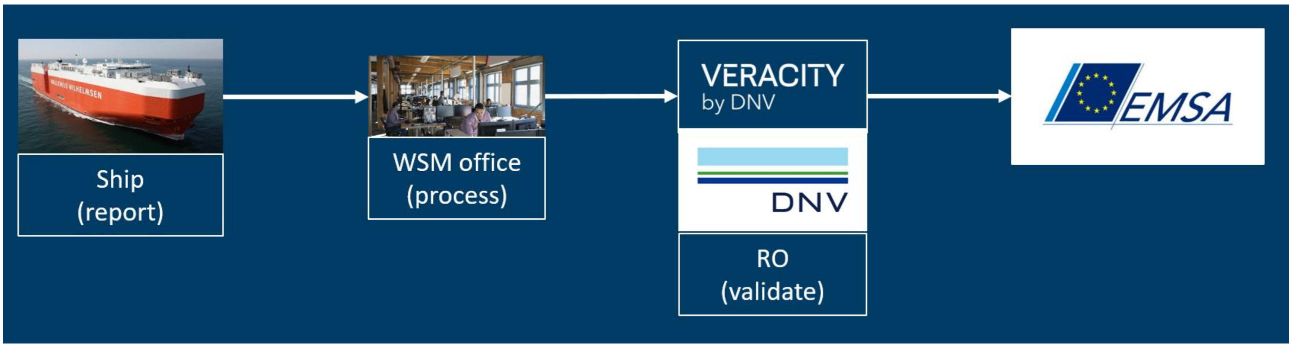


Figure 4 - EU MRV reporting before MDS project

NAVTOR, as a project owner, sees the increasing need for smooth data exchange between trusted maritime partners. This will facilitate new services supporting the required change to a safer, more efficient, and green shipping, also supporting IMO's strategy for GHG reductions by 50% within 2050. There are three main advantages realized through the Maritime Data Space in this business case: 1) Reduction of manual registration of data at the Wilhelmsen Ship Management office in Kuala Lumpur and the manual processing of data at their main office in Oslo. 2) Reduction of risk of human error as the manual registration and processing of data is automated. 3) DNV as Recognized Organization can respond much quicker to any potential flaws in the reporting, securing that measures may be taken immediately.

As a ship manager Wilhelmsen Ship Management operates a wide range of ship types on behalf of several owners. The reporting requirements are different from segment to segment and owner to owner. Another variable is the availability of sensor data which varies greatly between ships resulting in much of the data being manually collected and reported. New reporting requirements are typically solved with adding new data points that must be manually collected increasing the workload onboard. Furthermore, the cost of developing automatic or sensor-based reporting has been prohibitively expensive. The MDS concept fits perfectly to solve current challenges of information flow and reporting requirements. Through MDS data can be collected from multiple sources and aggregated to the appropriate format. This reduces the required effort both in data collection but also in quality assurance and post processing of data into the specific reporting format. In the test case of EU MRV reporting the effort of collecting data is reduced, as well as the effort needed for post processing and submittal to DNV.

<u>The data exchange process of Business Case 1 follows these steps (illustrated in Figure 5):</u>

1. Through the Maritime Data Space, the relevant data is captured onboard by the Neuron Solution Data Bridge and sent to Veracity for validation by DNV as the Recognized Organization (R.O.) on behalf of EMSA. Connectors from Neuron Solution and Veracity ensure that the data flows seamlessly from the ship to DNV.
2. Upon successful authentication, the data will be passed securely through Veracity as the trusted industry network for secure business collaboration. It will then be passed onwards via the DNV data warehouse that contains additional information also vital for the upcoming verification process. The Verification engine within the R.O. will compare emission reports with log abstracts from the vessel received via the Maritime Data Space. This will then be passed to the Nauticus Production System where the actual verification takes place.
3. The DNV Class Portal is the customers view, from which the customer will be presented with automatic verification results and is able to adjust these. When done, the data goes to the Verifier which is a manual step by the R.O. Finally, the verified report is sent the customer, who then can transmit the report to EU and IMO.

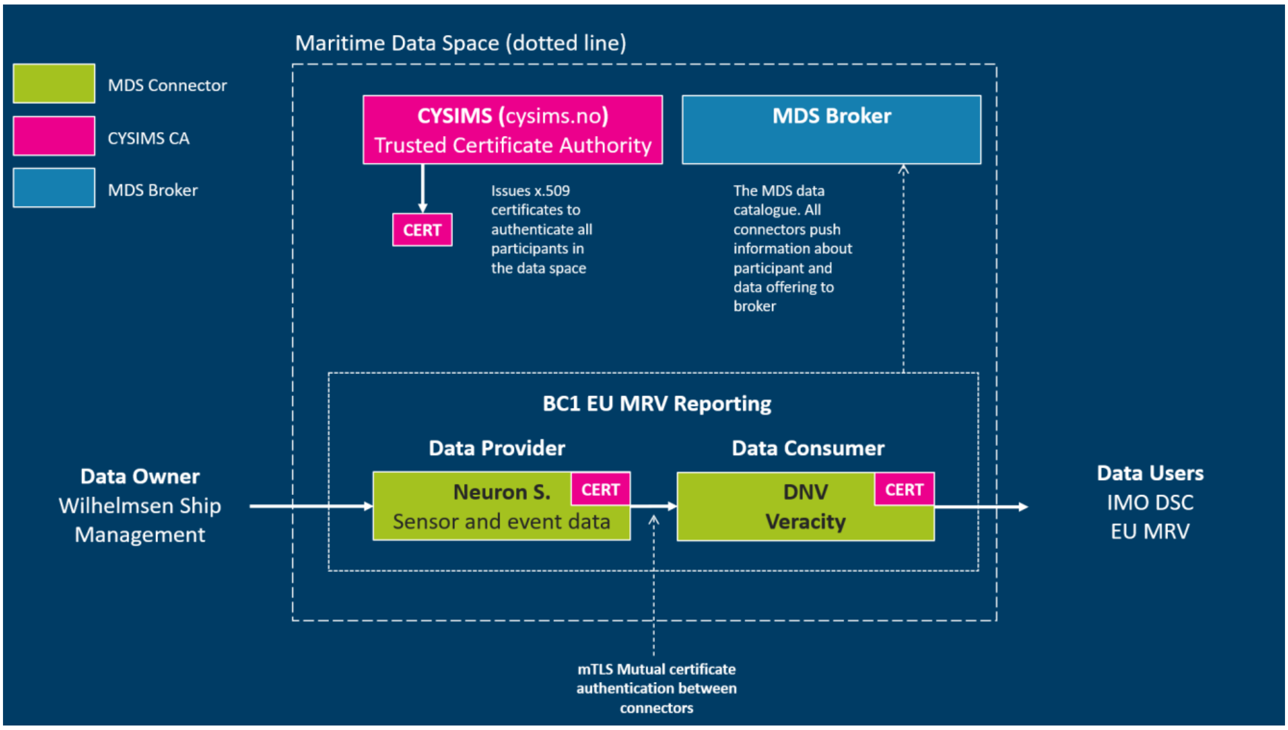
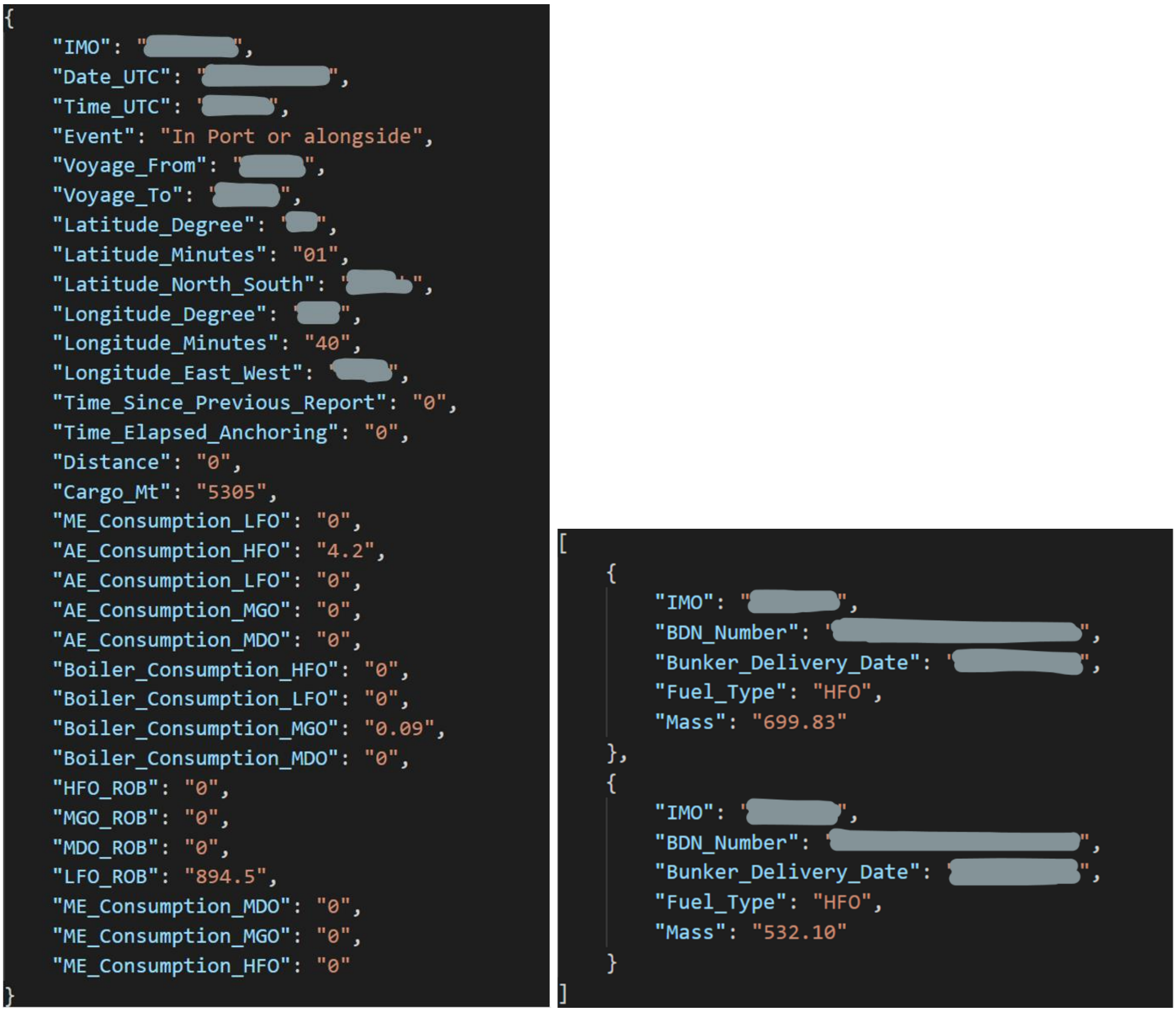

Maritime Data Space (dotted line)
MDS Connector
CYSIMS CA
MDS Broker
CYSIMS (cysims.no)
Trusted Certificate Authority
MDS Broker
CERT
Issues x.509 certificates to authenticate all participants in the data space
The MDS data catalogue. All connectors push information about participant and data offering to broker
BC1 EU MRV Reporting
Data Provider
Data Consumer
Data Owner
Wilhelmsen Ship Management
Neuron S.
Sensor and event data
CERT
DNV
Veracity
CERT
Data Users
IMO DSC
EU MRV
mTLS Mutual certificate authentication between connectors

Figure 5 - MDS Business Case 1: EU MRV Reporting

Figure 6 below shows an example of an actual response from the Neuron Solution provider connector which is consumed by the DNV connector.



```
{
    "IMO": "[redacted]",
    "Date_UTC": "[redacted]",
    "Time_UTC": "[redacted]",
    "Event": "In Port or alongside",
    "Voyage_From": "[redacted]",
    "Voyage_To": "[redacted]",
    "Latitude_Degree": "[redacted]",
    "Latitude_Minutes": "01",
    "Latitude_North_South": "[redacted]",
    "Longitude_Degree": "[redacted]",
    "Longitude_Minutes": "40",
    "Longitude_East_West": "[redacted]",
    "Time_Since_Previous_Report": "0",
    "Time_Elapsed_Anchoring": "0",
    "Distance": "0",
    "Cargo_Mt": "5305",
    "ME_Consumption_LFO": "0",
    "AE_Consumption_HFO": "4.2",
    "AE_Consumption_LFO": "0",
    "AE_Consumption_MGO": "0",
    "AE_Consumption_MDO": "0",
    "Boiler_Consumption_HFO": "0",
    "Boiler_Consumption_LFO": "0",
    "Boiler_Consumption_MGO": "0.09",
    "Boiler_Consumption_MDO": "0",
    "HFO_ROB": "0",
    "MGO_ROB": "0",
    "MDO_ROB": "0",
    "LFO_ROB": "894.5",
    "ME_Consumption_MDO": "0",
    "ME_Consumption_MGO": "0",
    "ME_Consumption_HFO": "0"
}
```

```
[
    {
        "IMO": "[redacted]",
        "BDN_Number": "[redacted]",
        "Bunker_Delivery_Date": "[redacted]",
        "Fuel_Type": "HFO",
        "Mass": "699.83"
    },
    {
        "IMO": "[redacted]",
        "BDN_Number": "[redacted]",
        "Bunker_Delivery_Date": "[redacted]",
        "Fuel_Type": "HFO",
        "Mass": "532.10"
    }
]
```

Figure 6 - Example data fields from EU MRV reporting (left: 'Log Abstract report', right: 'Bunker report')

4.2 Business Case 2 – Vessel Speed/ ETA Management

The ETA (Estimated Time of Arrival) Management business case is a new service made available by the Maritime Data Space. ETA and speed management is an important enabler for both emission management and cost savings. NAVTOR provides a type of approved Gateway called NAVBOX, facilitating secure data exchange. The commercial operator of the vessels under Wilhelmsen's technical management uses the same data elements in their day-to-day operation but with lower resolution/ frequency. Through the Maritime Data Space, the NAVTOR API can send data on the same level of accuracy/ detail as used in NAVTOR's web-based fleet monitoring service, NavFleet, directly to Wilhelmsen Ship Management. Wilhelmsen Ship Management can then add analytics to this data and give the operator access to more real-life analysis and decision support.

There are three main advantages realized through the Maritime Data Space in this business case: 1) Wilhelmsen Ship Management receives more detailed and accurate data to be used in their ETA Management, 2) The data used in the ETA Management is now consistent with actual navigational data and 3) The response time from identifying any deviation from the ETA Management Plan is reduced.

Wilhelmsen Ship Management can add analytics to operational data and provide the operator with more accurate data to be used in their ETA Management.

For NAVTOR, the MDS project has established a framework for data sharing that will facilitate NAVTOR's increasing data exchange vessel-shore, and contribute to new services in three ways;

- **First**, by sharing vessel information, like Passage-Plan data, with customers and partners via API, making sure there is consistency between provided data and data being displayed in NAVTOR's systems on board and on shore.
- **Secondly,** by adding new services to the onboard planning station NavStation, like near real time monitoring of fuel consumption supported by shore-based analytics, and
- **Third;** MDS data sharing will contribute to the fundament for shore-based monitoring of Safety and Fuel Performance in the new Fleet monitoring service NavFleet - launched in Spring 2021.

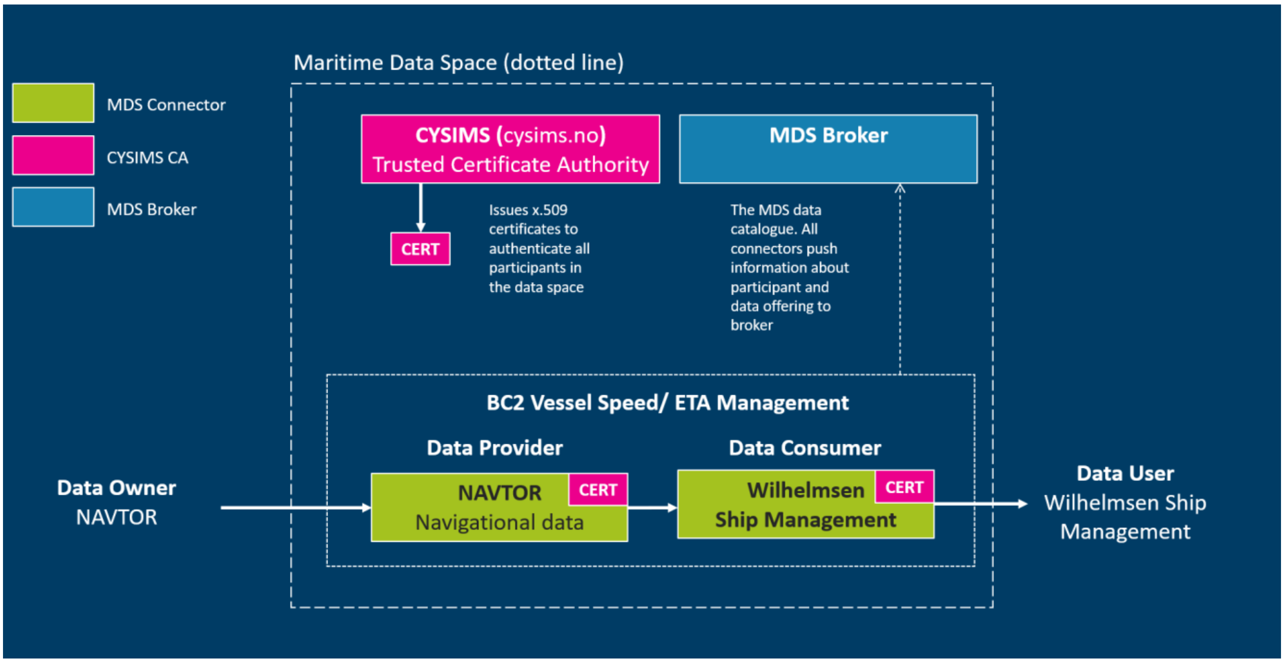
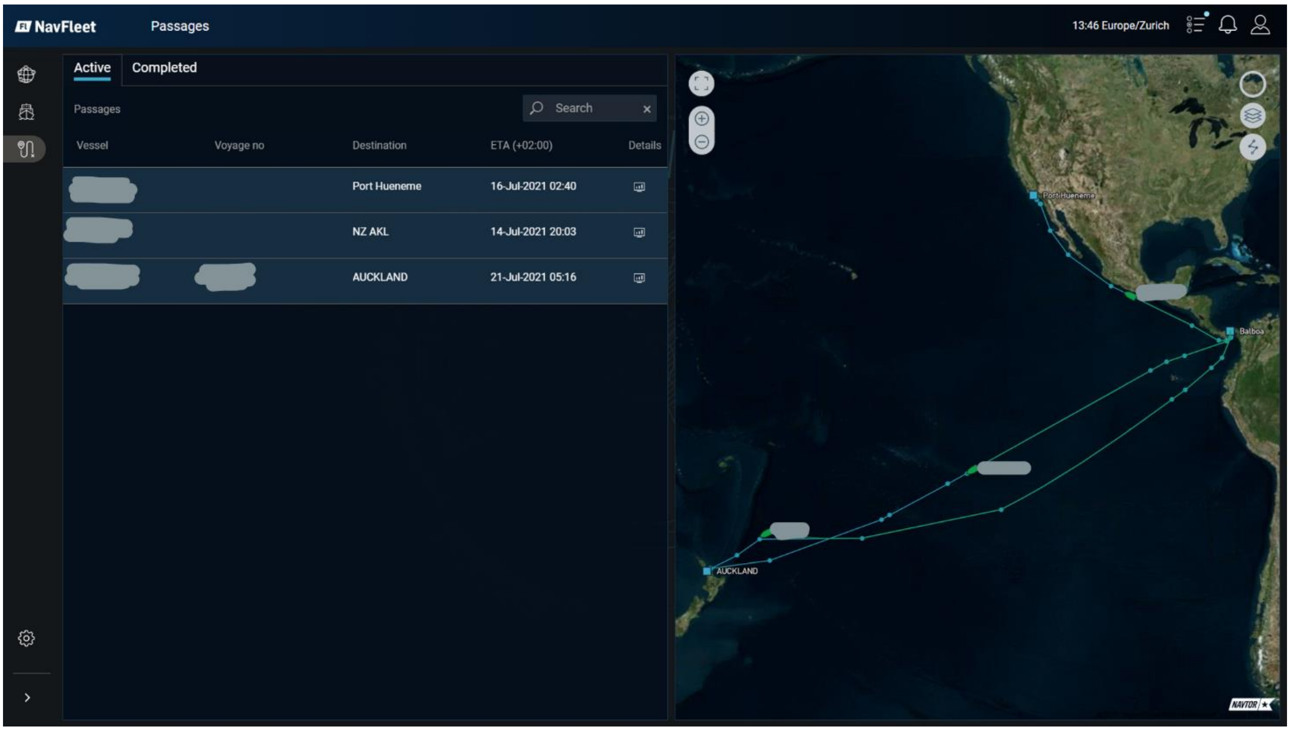

Maritime Data Space (dotted line)
MDS Connector
CYSIMS CA
MDS Broker
CYSIMS (cysims.no)
Trusted Certificate Authority
MDS Broker
CERT
Issues x.509 certificates to authenticate all participants in the data space
The MDS data catalogue. All connectors push information about participant and data offering to broker
BC2 Vessel Speed/ ETA Management
Data Provider
Data Consumer
Data Owner
NAVTOR
NAVTOR
Navigational data
CERT
Wilhelmsen
Ship Management
CERT
Data User
Wilhelmsen Ship Management

Figure 7 - MDS Business Case 2: ETA Management



NavFleet Passages 13:46 Europe/Zurich

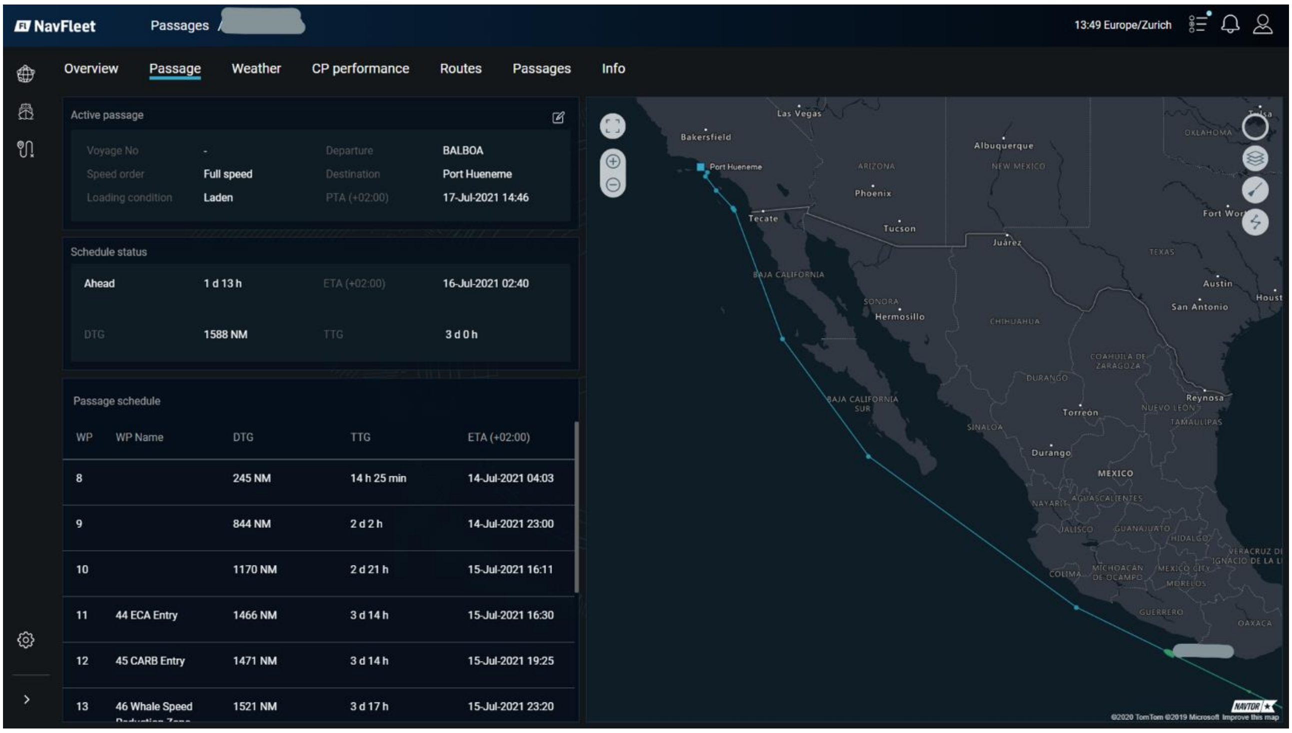
Active | Completed

Passages

Vessel	Voyage no	Destination	ETA (+02:00)	Details
[redacted]		Port Hueneme	16-Jul-2021 02:40	
[redacted]		NZ AKL	14-Jul-2021 20:03	
[redacted]	[redacted]	AUCKLAND	21-Jul-2021 05:16	

Figure 8 - NAVTOR NavFleet ETA Management

Figure 8 above shows actual data and visualizations of ETA Management for three different vessels that all have installed NAVTOR's planning module onboard. Figure 9 shows DTG (Distance To Go), TTG (Time To Go) and ETA (Estimated Time of Arrival) for a specific vessel.



NavFleet Passages / [redacted] 13:49 Europe/Zurich

Overview | Passage | Weather | CP performance | Routes | Passages | Info

Active passage

Voyage No	-	Departure	BALBOA
Speed order	Full speed	Destination	Port Hueneme
Loading condition	Laden	PTA (+02:00)	17-Jul-2021 14:46

Schedule status

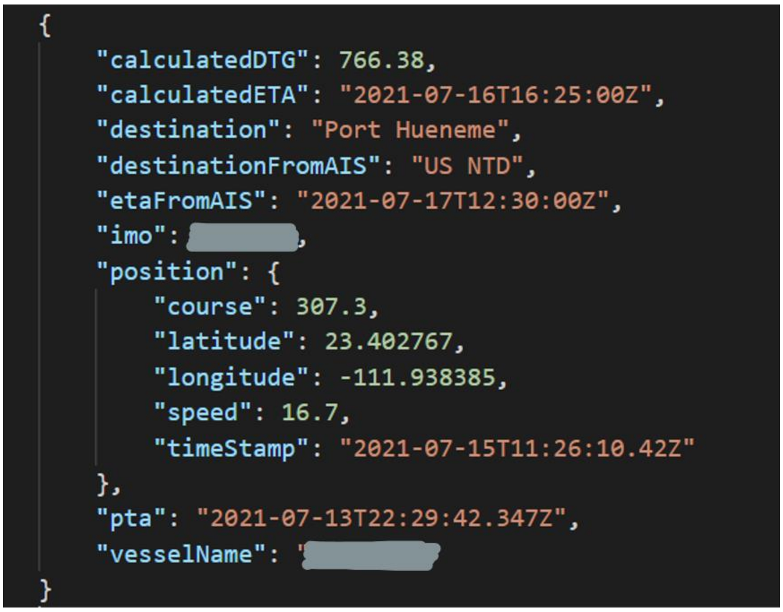
Ahead	1 d 13 h	ETA (+02:00)	16-Jul-2021 02:40
DTG	1588 NM	TTG	3 d 0 h

Passage schedule

WP	WP Name	DTG	TTG	ETA (+02:00)
8		245 NM	14 h 25 min	14-Jul-2021 04:03
9		844 NM	2 d 2 h	14-Jul-2021 23:00
10		1170 NM	2 d 21 h	15-Jul-2021 16:11
11	44 ECA Entry	1466 NM	3 d 14 h	15-Jul-2021 16:30
12	45 CARB Entry	1471 NM	3 d 14 h	15-Jul-2021 19:25
13	46 Whale Speed	1521 NM	3 d 17 h	15-Jul-2021 23:20

Figure 9 - NAVTOR NavFleet ETA Management for a specific vessel

Figure 10 shows an example of the data fields that are available for Wilhelmsen Ship Management to consume in business case 2 of the MDS project.



```
{
    "calculatedDTG": 766.38,
    "calculatedETA": "2021-07-16T16:25:00Z",
    "destination": "Port Hueneme",
    "destinationFromAIS": "US NTD",
    "etaFromAIS": "2021-07-17T12:30:00Z",
    "imo": [redacted],
    "position": {
        "course": 307.3,
        "latitude": 23.402767,
        "longitude": -111.938385,
        "speed": 16.7,
        "timeStamp": "2021-07-15T11:26:10.42Z"
    },
    "pta": "2021-07-13T22:29:42.347Z",
    "vesselName": [redacted]
}
```

Figure 10 - Data fields available from NAVTOR NavFleet

4.3 Business Case 3 – Ship Reporting

Automatic MRS-reporting to the Norwegian Coastal Administration. Mandatory Ship Reporting, in the Norwegian Coastal Administration's case through the Maritime Single Window (SSN NO) is a reporting regime for ships entering Norwegian waters. In this business case (Figure 11), NAVTOR captures the required data from the ship through Neuron Solutions' MDS connector, processes the data and generates the required MRS message. A request for the PKI signature is sent to the PKI unit which signs the message and sends it back to NAVTOR for submission through the Norwegian Coastal Administration's Maritime Single Window. The Norwegian Coastal Administration verifies the signature using the PKI-unit and approves/rejects the message. Through the MDS ecosystem, in combination with the CySiMS PKI solution, NAVTOR is able to capture required data from the ship and sign the MRS message (Figure 12). The Norwegian Coastal Administration is able to verify the sender of the MRS.

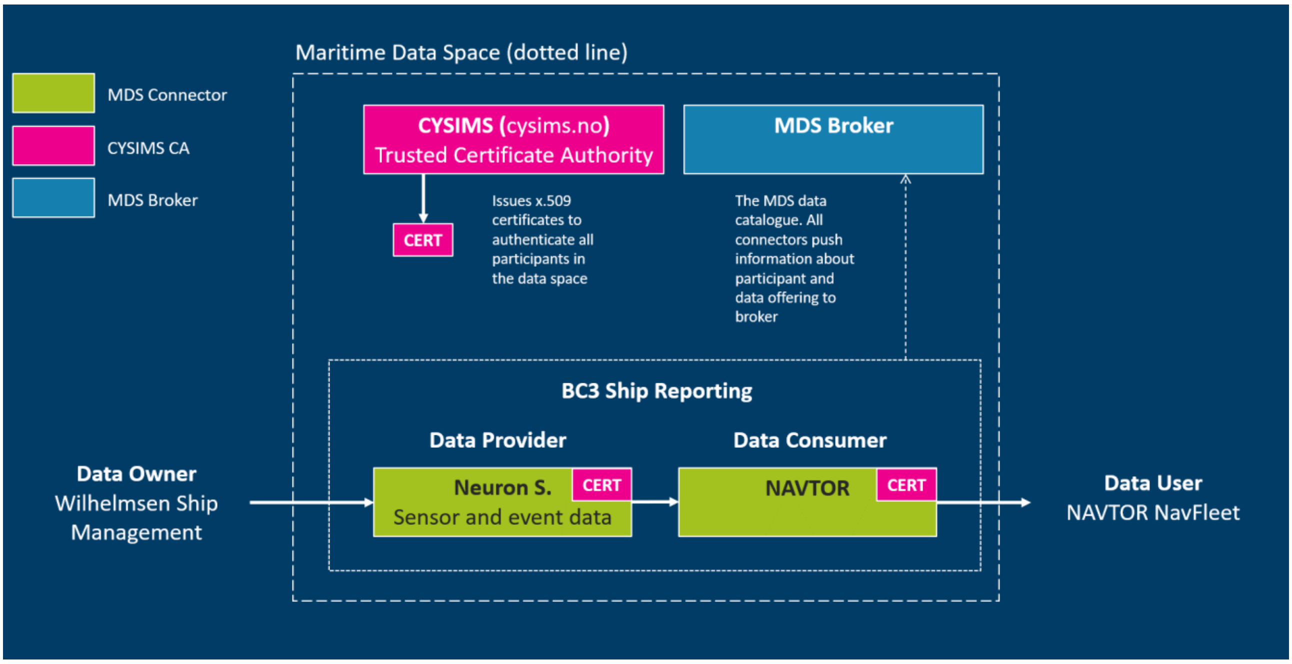

MDS Connector
CYSIMS CA
MDS Broker
Maritime Data Space (dotted line)
CYSIMS (cysims.no)
Trusted Certificate Authority
MDS Broker
CERT
Issues x.509 certificates to authenticate all participants in the data space
The MDS data catalogue. All connectors push information about participant and data offering to broker
BC3 Ship Reporting
Data Provider
Data Consumer
Data Owner
Wilhelmsen Ship Management
Neuron S.
Sensor and event data
CERT
NAVTOR
CERT
Data User
NAVTOR NavFleet

Figure 11 - MDS Business Case 3: Ship Reporting

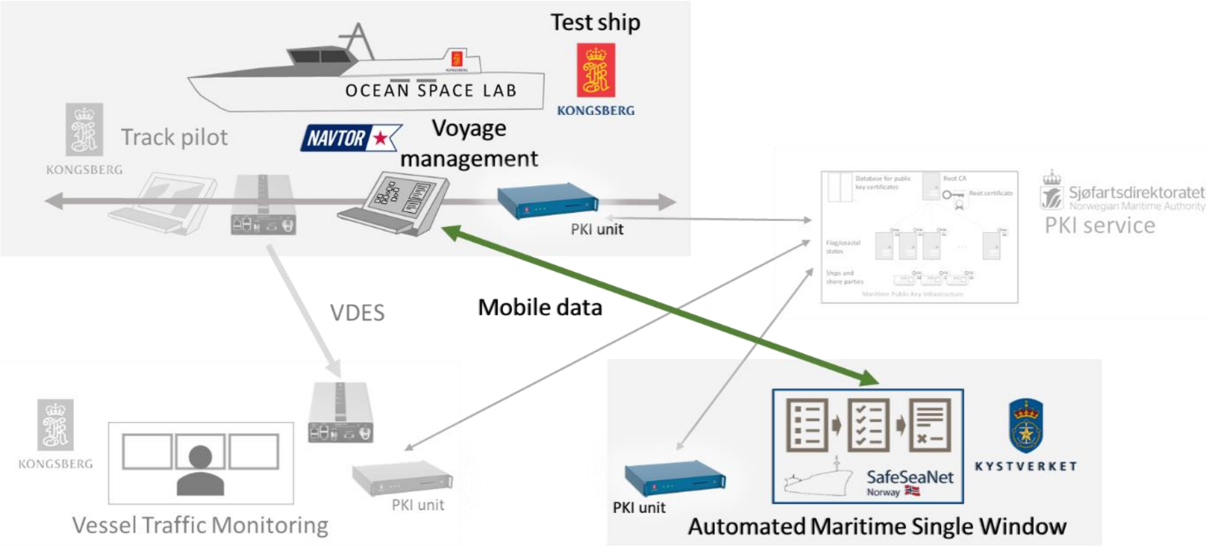


Figure 12 - Automatic MRS-reporting (create and verify signature)

5 MDS Functional Layer

The Functional Layer defines the functional requirements of the Data Space, including the functionality and features to be implemented. Figure 13 shows the functional architecture outlined by IDSA. The remainder of this section will discuss how the Maritime Data Space is aligned with the functional requirements defined by IDSA, as described in the table below.

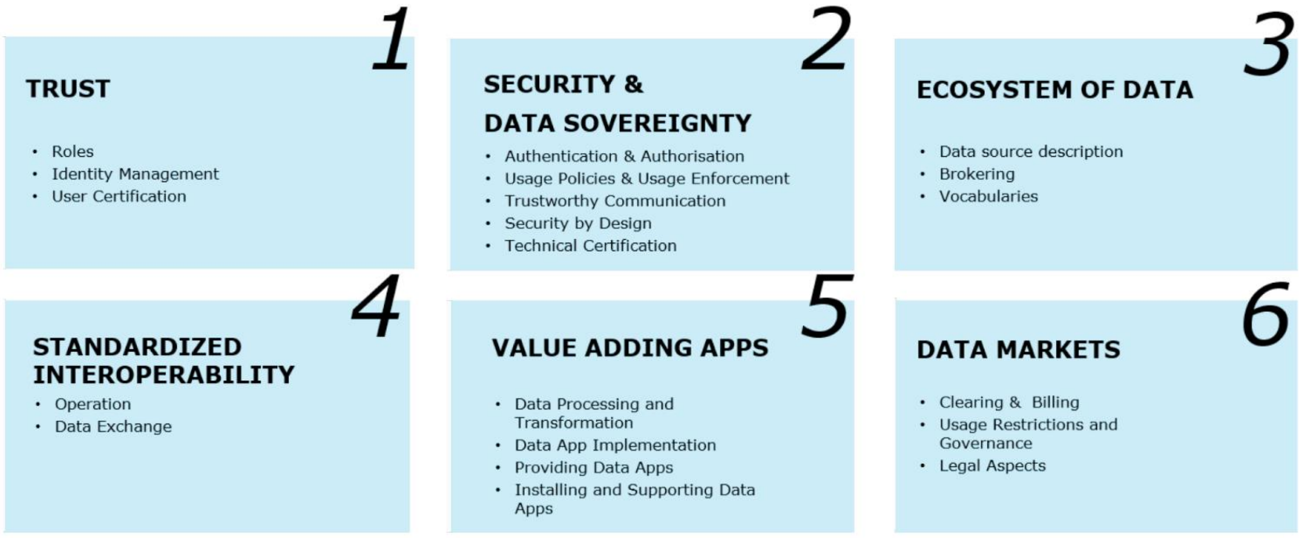

1
TRUST
• Roles
• Identity Management
• User Certification
2
SECURITY &
DATA SOVEREIGNTY
• Authentication & Authorisation
• Usage Policies & Usage Enforcement
• Trustworthy Communication
• Security by Design
• Technical Certification
3
ECOSYSTEM OF DATA
• Data source description
• Brokering
• Vocabularies
4
STANDARDIZED INTEROPERABILITY
• Operation
• Data Exchange
5
VALUE ADDING APPS
• Data Processing and Transformation
• Data App Implementation
• Providing Data Apps
• Installing and Supporting Data Apps
6
DATA MARKETS
• Clearing & Billing
• Usage Restrictions and Governance
• Legal Aspects

Figure 13 - Functional architecture outlined by IDSA

Functional Layer Aspect	IDSA Requirement	MDS Implementation
1 TRUST		
Roles	Each role in the International Data Spaces has certain rights and duties. As an example, the Identity Provider is responsible for offering services to create, maintain, manage, monitor, and validate identity information of and for participants in the International Data Spaces.	**Identity Provider:** CySIMS PKI **BC1/ BC3 data owner:** Wilhelmsen, **BC1/ BC3 data provider:** Neuron Solution, **BC1 data consumer:** DNV. **BC2 data owner:** Wilhelmsen. **BC2 data provider:** NAVTOR, **BC2 data consumer:** Wilhelmsen, **BC3 data consumer:** NAVTOR
Identity Management	Every Connector participating in the International Data Spaces must have a unique identifier and a valid certificate. In addition, each Connector must be able to verify the identity of other Connectors.	All MDS provider and consumer connectors are uniquely identified by an X.509 certificate issued by the trusted MDS Certificate Authority CySIMS.
2 SECURITY AND DATA SOVEREIGNTY		
Authentication and Authorization	Each Connector must have a valid X.509 certificate. With the help of this certificate, each participant in the International Data Spaces that operates an endpoint can verify the identity of any other participant. Certain conditions (e.g.,	All MDS provider and consumer connectors are uniquely identified by an X.509 certificate issued by the trusted MDS Certificate Authority CySIMS. Connectors use mTLS (mutual Transport Layer Security) to communicate. Secure communication in all business cases based on

	security profiles) may also apply here. The Connector serving as the data source must be able to verify the receiving Connector's capabilities and security features as well as its identity.	two-way authentication. All MDS participants are assigned a custom domain. Each certificate is again linked to this unique domain, and this forms the basis of the MDS trust ecosystem. The unique thumbprint of each certificate is used to allow and restrict access to data offerings.
Usage Policies and Usage Enforcement	Data Owners and Data Providers can always be sure their data is handled by a Data Consumer according to the usage policies specified. Each participant can define usage policies and attach them to outbound data. Policies might include restrictions, such as disallowing persistence of data, or disallowing transfer of data to other parties	Usage policies in MDS are not enforced technically, but rather described in the information model of each connector. Data usage is handled on a contractual level between participants. Connectors expose an endpoint where this information is available.
Trustworthy Communication	Connectors, App Stores, and Brokers can check if the Connector of the connecting party is running a trusted (i.e., certified) software stack. Any communication between (external) Connectors can be encrypted and integrity protected. Each Data Owner and Data Provider must be able to ensure that their data is handled by the Connector of the Data Consumer according to the usage policies specified: otherwise, the data will not be sent.	The communication between connectors is encrypted over HTTPS by use of mutual Transport Layer Security (mTLS) and X.509 certificates issued by the trusted CA CySIMS. mTLS requires both the provider connector and the consumer connector to verify each other through a handshake to establish communication.
Technical Certification	The core components of the International Data Spaces, and especially the Connectors, require certification from the Certification Body to establish trust among all participants.	Certification falls outside of the scope of the MDS project.
3 ECOSYSTEM OF DATA		
Data source Description	Participants must have the opportunity to describe, publish, maintain, and manage different versions of metadata. Metadata should describe the syntax and serialization as well as the semantics of data sources. Furthermore, metadata should describe the application domain of the data source. The operator of a Connector must be able to define the price, the pricing model, and the usage policies regarding certain data.	MDS connectors can describe metadata about participants and data offerings through the API endpoint /metadata. The metadata description follows the IDSA information model along the dimensions of content, concept, context, commodity, community of trust and communication.
Brokering	The operator of a Connector must be able to provide an interface for data and metadata access. Each Connector must be able to transmit metadata of its data sources to one or more brokers. Each participant must be able to browse and search metadata in the metadata repository, provided the participant has	The MDS project has developed a proof of concept at maturity level TRL4 that demonstrates the capabilities of a Broker service. The Broker can collect metadata from each connector that describes itself and its data offerings via the API endpoint /metadata.

	the right to access the metadata. Furthermore, each participant must be able to browse the list of participants registered at a broker.	
4 STANDARDIZED INTEROPERABILITY		
Operation	Participants should be able to run the Connector software in their own IT environment. Alternatively, they can run a Connector on mobile or embedded devices. The operator of the Connector must be able to define the data workflow inside the Connector.	Both data provider and consumer connectors in MDS run in different deployment/ production settings based on the needs in each business case. Most connectors run in Azure as a web service. As an example, the DNV consumer connector in business case 1 runs in Veracity's own deployment environment as an Azure web service that feeds data to internal services at DNV Maritime.
Data Exchange	The Connector must receive data from an enterprise backend system, either through a push-mechanism or a pull-mechanism. The data can be provided via an interface or pushed directly to other participants. To do so, each Connector must be uniquely identifiable. Other Connectors can subscribe to data sources or pull data from these sources. Data can be written into the backend system of other participants.	MDS data providers in all business cases **push** data to the provider connectors. In turn, data consumers in all three business cases **pull** data from the provider connectors via the consumer connectors.

6 MDS Information Layer

The Information Layer specifies the Information Model which is the domain-agnostic, common language of the International Data Spaces. The Information Model is an essential agreement shared by the participants and components of the IDS, facilitating compatibility and interoperability. The primary purpose of this formal model is to enable (semi-)automated exchange of digital resources within a trusted ecosystem of distributed parties, while preserving data sovereignty of Data Owners. The Information Model therefore supports the description, publication and identification of data products and reusable data processing software. The communication between technological components in MDS relies on the use of the Information Model, and the MDS connectors include functionality to describe both the participant and the data offering according to the concern hexagon illustrated in Figure 14 below.

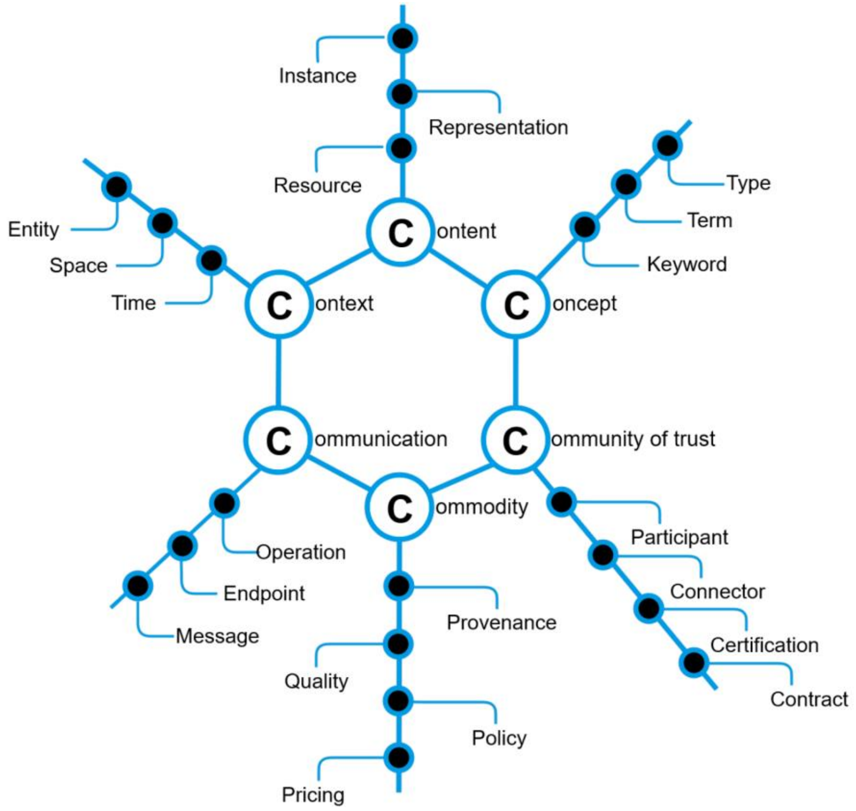


Figure 14 - Information Model, conceptual representation

7 MDS System Layer

The System Layer describes the logical software components, considering aspects such as integration, configuration, and deployment. This layer can be considered the technical implementation layer of a Data Space that will be defined by mapping roles from the Business Layer and technical requirements from the Functional Layer to a concrete data and service architecture in the System Layer. From the requirements on the Functional Layer, three major technical components result: **1) The Certificate Authority, 2) The Connectors, and 3) The Broker.**

The **Connector** is responsible for the exchange of data or as a proxy in the exchange of data, as it executes the complete data exchange process from and to the internal data resources and enterprise systems of the participating organizations. The Connector provides metadata to the Broker about its technical interface description, authentication mechanism, exposed data sources, and associated data usage policies. It is important to note that the data is transferred directly between the Connectors of the Data Provider and the Data Consumer according to a decentralized peer-to-peer network concept. Hence, there is no centralized technical component in the Data Space that mediates data exchange between participants.

The Connector architecture uses application container management technology to ensure an isolated and secure environment for individual data services. Figure 19 in Section 7.2 illustrates the internal structure of the Connector. An actual use case specific installation of a Connector may differ from this reference implementation, as existing components can be modified, and optional components added.

7.1 The MDS CySIMS Certificate Authority (CA)

This private GitHub repository contains alle needed information to set up the CySIMS Certificate Authority in the Maritime Data Space project:

(private repository available for MDS project partners)
https://github.com/maritime-data-space/cysims-certificate-authority

The repository contains certificates and configuration files for establishing a Certificate Authority (CA) for the Maritime Data Space project. The setup for establishing a new CA can be reused in any other ecosystem for data sharing based on the specifications of the International Data Spaces Association (IDSA).

- The Maritime Data Space (MDS) ecosystem has established a Certificate Authority (CA) that complies with the Reference Architecture Model 3.0 issued by the International Data Spaces Association (IDSA).
- The CA (Figure 16) issues X.509 certificates for all entities and actors involved in MDS. These certificates are used for authentication and encryption between Connectors and are also used to authorize user access to data being offered by data providers.
- The authentication mechanisms of MDS (Figure 17) verify that the users are who they say they are, while the authorization process (Figure 18) gives authenticated users permission to access certain resources.
- The specific implementation of the MDS CA follows the Public Key Infrastructure (PKI) specification created by the CySiMS innovation project. The specification can be found in the 'resources' folder of the GitHub repository. The underlying idea of CySiMS is to develop new maritime security solutions that provide integrated and cost-effective protection against cyber-attacks on critical safety and operational information, while contributing to and making use of emerging specifications and standards. The realization of a public key infrastructure for the maritime domain has been one of the results of this project. Partners in CySiMS include Navtor, SINTEF Digital and SINTEF Ocean, Kongsberg, Norwegian Maritime Authority, and The Norwegian Coastal Administration.
- The CA that has been established for the MDS ecosystem uses a three-level trust hierarchy (Figure 15) in which the top-level Root CA and the Intermediate CA have been operated by SINTEF Digital for demonstration purposes within the scope of the MDS project. The public key certificates have been issued to end entities (i.e., the connectors) in the MDS ecosystem that need to communicate securely. Each provider and consumer connector in all three MDS business cases has implemented an X.509 certificate issued by the Root and Intermediate CA.
- All public key certificates in the MDS ecosystem will be X.509 v3 certificates encoded in PEM format. The public key certificate values are in accordance with the RFC 5480 standard for Elliptic Curve Cryptography.

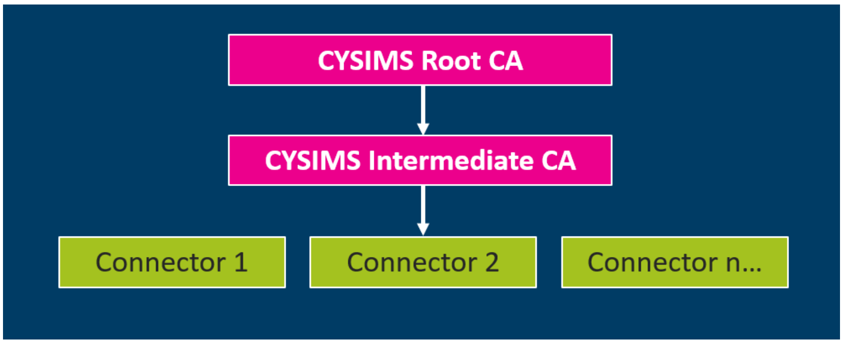
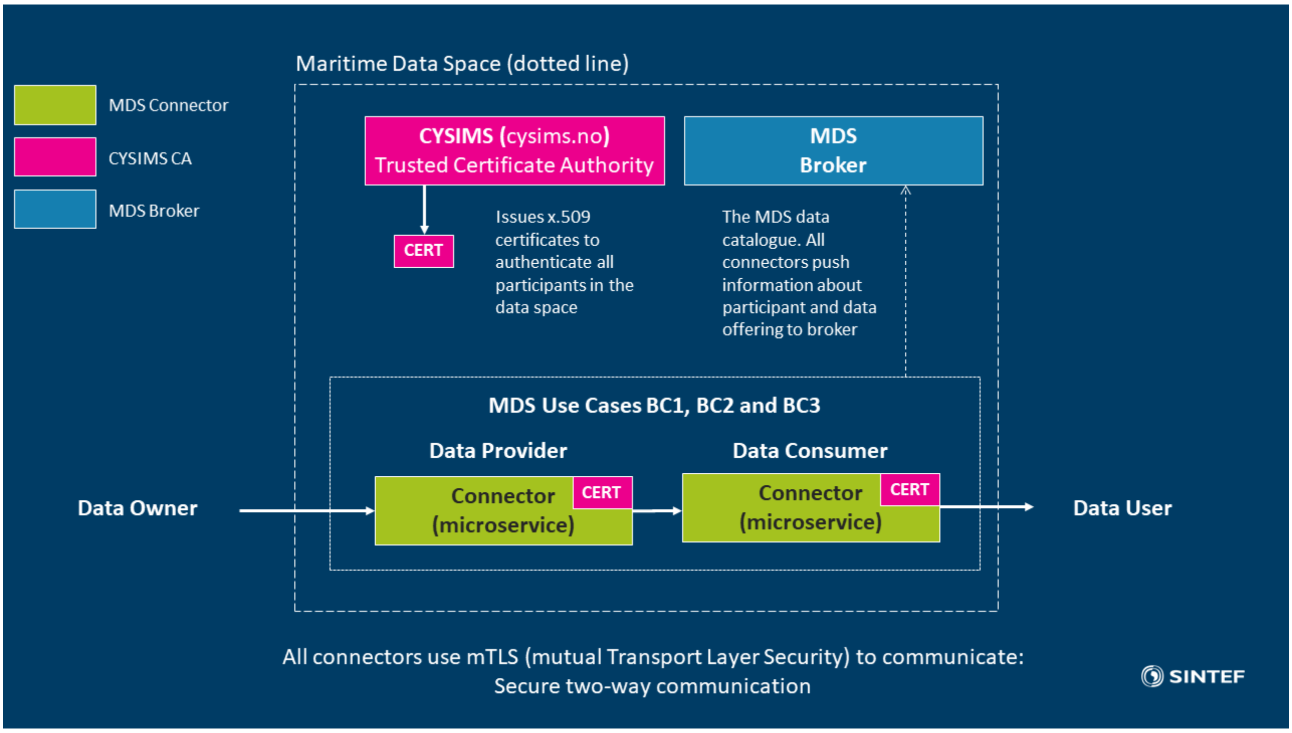


Figure 15 - MDS trust hierarchy



🟩 MDS Connector

🟥 CYSIMS CA

🟦 MDS Broker

Maritime Data Space (dotted line)

CYSIMS (cysims.no)
Trusted Certificate Authority

CERT

Issues x.509 certificates to authenticate all participants in the data space

MDS
Broker

The MDS data catalogue. All connectors push information about participant and data offering to broker

MDS Use Cases BC1, BC2 and BC3

Data Provider

Data Consumer

Data Owner

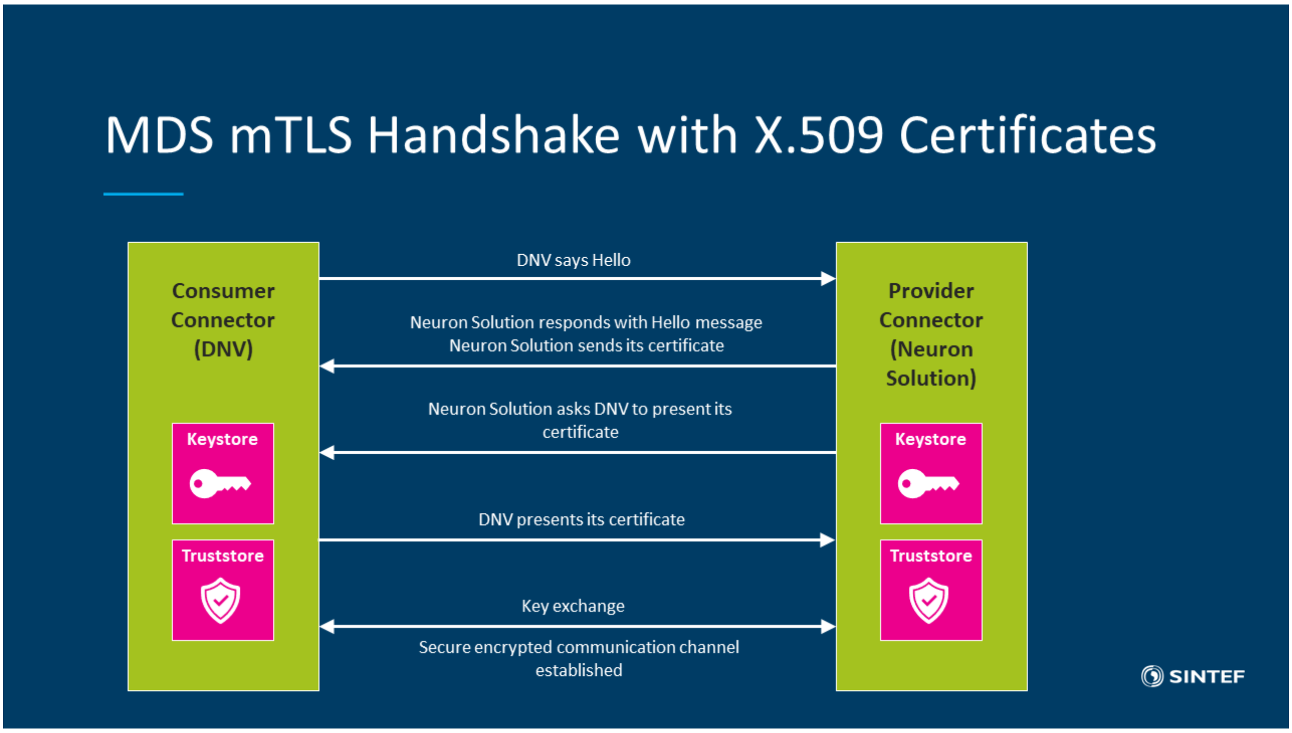
Connector (microservice) CERT

Connector (microservice) CERT

Data User

All connectors use mTLS (mutual Transport Layer Security) to communicate:
Secure two-way communication

Figure 16 - The CySIMS Certificate Authority in MDS



MDS mTLS Handshake with X.509 Certificates

Consumer Connector (DNV)

Keystore

Truststore

Provider Connector (Neuron Solution)

Keystore

Truststore

DNV says Hello

Neuron Solution responds with Hello message
Neuron Solution sends its certificate

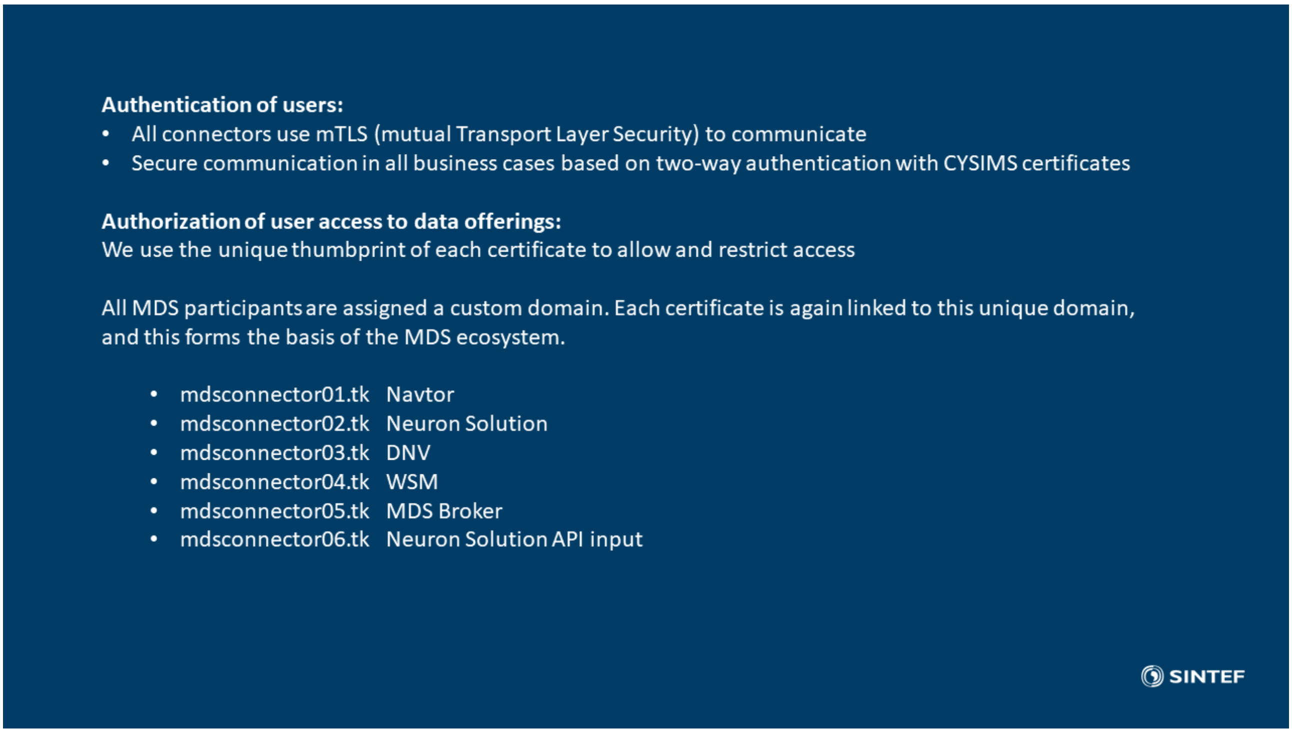
Neuron Solution asks DNV to present its certificate

DNV presents its certificate

Key exchange

Secure encrypted communication channel established

Figure 17 - mTLS handshake between MDS Connectors



Authentication of users:

- All connectors use mTLS (mutual Transport Layer Security) to communicate
- Secure communication in all business cases based on two-way authentication with CYSIMS certificates

Authorization of user access to data offerings:
We use the unique thumbprint of each certificate to allow and restrict access

All MDS participants are assigned a custom domain. Each certificate is again linked to this unique domain, and this forms the basis of the MDS ecosystem.

• mdsconnector01.tk	Navtor
• mdsconnector02.tk	Neuron Solution
• mdsconnector03.tk	DNV
• mdsconnector04.tk	WSM
• mdsconnector05.tk	MDS Broker
• mdsconnector06.tk	Neuron Solution API input

SINTEF

Figure 18 - MDS authentication, authorization, and custom domains

This section presents the establishment of the PKI (i.e., Root CA, Intermediate CA, and end entity certificates) using OpenSSL. The steps to establish the PKI are the following:

1. Generate the Root CA public key certificate (self-signed)
2. Generate the Intermediate CA public key certificate, signed by the Root CA
3. Generate an end entity certificate for a connector, signed by the Intermediate CA

The following sections presents the OpenSSL commands that will be executed to do this. *The file paths in each command refer to the folder structure of the CA GitHub repository.*

7.1.1 Create Root CA

Public private key pair for Root CA

```
openssl genpkey -algorithm EC -aes128 -pass file:passphrase.txt -pkeyopt ec_paramgen_curve:P-384 -
out ca.domain.key.pem
```

Self-signing the Root CA public key certificate

```
openssl req -config ./03_configuration_files/ca_root.cnf -new -x509 -sha256 -extensions v3_ca -key
ca.domain.key.pem -out ca.domain.crt.pem -days 7300 -subj
"/C=NO/O=NorwegianMaritimeAuthority/CN=CysimsRootCA"
```

7.1.2 Create Intermediate CA

Public private key pair for Intermediate CA

```
openssl genpkey -algorithm EC -aes128 -pass file:passphrase.txt -pkeyopt ec_paramgen_curve:P-384 -
out ca_intermediate.domain.key.pemca.domain.key.pem
```

Generating CSR (Certificate Signing Request) for Intermediate CA

```
openssl req -config ./03_configuration_files/ca_root.cnf -new -key ca_intermediate.domain.key.pem -
out ca_intermediate.domain.csr -subj
"/C=NO/O=NorwegianMaritimeAuthority/CN=CysimsIntermediateCA-0"
```

Using the Root CA to sign Intermediate CA certificate

```
openssl ca -config ./03_configuration_files/ca_root.cnf -extensions v3_intermediate_ca -days 3650 -
notext -in ca_intermediate.domain.csr -out ca_intermediate.domain.crt.pem
```

Verifying the Intermediate CA public key certificate

```
openssl verify -CAfile ca.domain.crt.pem ca_intermediate.domain.crt.pem
```

7.1.3 Create End Entity Certificate

Public private key pair generation

```
openssl genpkey -algorithm EC -aes128 -pass file:passphrase.txt -pkeyopt ec_paramgen_curve:P-256 -
out navtor.domain.key.pem
```

Generating the CSR to be signed by Intermediate CA

```
openssl req -new -key navtor.domain.key.pem -out navtor.domain.csr.pem -subj
"/CN=mdsconnector01.tk/C=NO/O=NorwegianMaritimeAuthority/OU=MDS.NAVTOR"
```

SERVER end user certificate: Using Intermediate CA to sign the CSR

```
openssl ca -config ./configuration_files/ca_intermediate.cnf -extensions server_cert -days 1095 -notext
-md sha256 -in navtor.domain.csr.pem -out navtor.domain.crt.pem
```

CLIENT end user certificate: Using Intermediate CA to sign the CSR

```
openssl ca -config ./configuration_files/ca_intermediate.cnf -extensions client_cert -days 1095 -notext -
md sha256 -in navtor.domain.csr.pem -out navtor.domain.crt.pem
```

Verifying the end entity public key certificate using CA chain bundle

```
openssl verify -CAfile ca-chain-bundle.cert.pem navtor.domain.crt.pem
```

7.1.4 Steps to export certificates to keystore

OpenSSL and Keytool are used to export certificates to a keystore, and convert between different keystore formats (i.e., PFX and JKS).

Export to PFX keystore

```
openssl pkcs12 -export -out navtor.pfx -inkey navtor.domain.key.pem -in navtor.domain.crt.pem
```

Convert PFX to JKS

```
keytool -importkeystore -srckeystore navtor.pfx -srcstoretype pkcs12 -destkeystore navtor.jks -
deststoretype JKS
```

Change alias name

```
keytool -changealias -keystore navtor.jks -alias 1 -destalias navtor
```

Import Root CA to keystore

```
keytool -import -alias root -keystore navtor.jks -trustcacerts -file ca_root/ca.domain.crt.pem
```

Import intermediate CA to keystore

```
keytool -import -alias intermediate -keystore navtor.jks -trustcacerts -file
ca_intermediate/ca_intermediate.domain.crt.pem
```

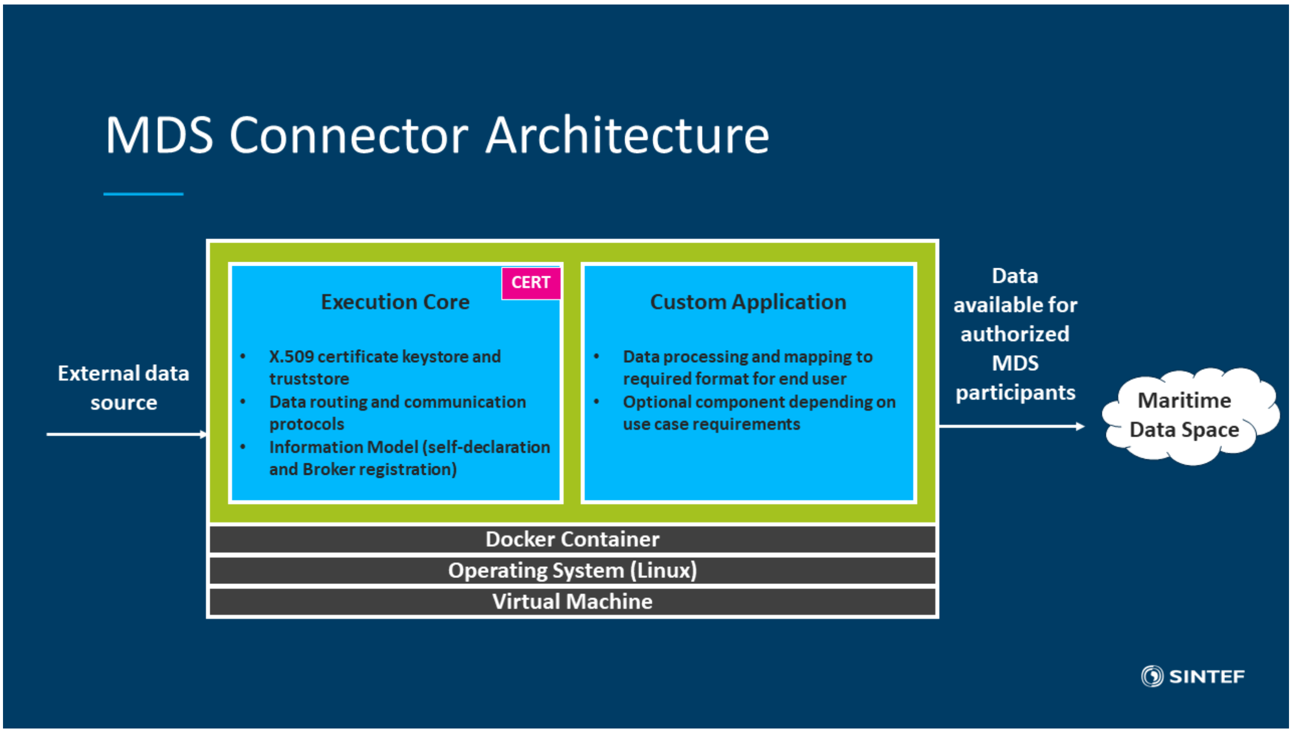
Export to PFX keystore from JKS keystore

```
keytool -importkeystore -srckeystore wsm_client.jks -destkeystore wsm_client.pfx -srcstoretype JKS -
deststoretype PKCS12
```

7.2 The MDS Connectors and Broker Service Implementations

These repositories contain connector and broker services for the Maritime Data Space based on the specifications of the International Data Spaces Association (IDSA). The MDS specific implementations are described in more detail in the following repositories:

- https://github.com/maritime-data-space/connectors-broker (private repository)
- https://github.com/veracity/MDSConnector (public repository)



MDS Connector Architecture

External data source
Execution Core
CERT
X.509 certificate keystore and truststore
Data routing and communication protocols
Information Model (self-declaration and Broker registration)
Custom Application
Data processing and mapping to required format for end user
Optional component depending on use case requirements
Docker Container
Operating System (Linux)
Virtual Machine
Data available for authorized MDS participants
Maritime Data Space
SINTEF

Figure 19 - Reference Connector architecture in MDS

The **Execution Core** of the Connector includes the following components:

- **Application Container Management:** Data services are isolated from each other by containers (e.g., Docker) to prevent unintended interdependencies.
- **X.509 certificate keystore and trust store**
- **Execution Core Container:** Provides components for interfacing with data services through a Data Router or Data Bus. A Data Router or a Data Bus handle communication with data services to be invoked according to predefined configuration parameters.
- **Information Model** that describes participant and data offerings and exposes an API endpoint for the Broker to consume.

OPTIONAL: The **Custom Application** of the Connector includes the following components:

- **Custom Container:** Provides a data service developed by a participant. Custom containers usually require no certification.

8 Cross-sectional Perspectives in MDS: Security, Certification and Governance

The general structure of the Reference Architecture Model consists of five layers, as described in section 2: 1) The Business Layer, 2) The Functional Layer, 3) The Process Layer, 4) The Information Layer, and 5) The System Layer. In addition, the Reference Architecture Model comprises three perspectives that need to be implemented across all five layers: *Security, Certification, and Governance.*

8.1 Security Perspectives

The Security Architecture in MDS follows two general principles that are aligned with the IDSA Reference Architecture Model:

- **Use of existing standards and best practices for security** approaches and solutions that have been implemented in MDS. The Security Architecture combines existing, reliable approaches in a useful and meaningful way.
- **Scalability of security levels:** MDS does not enforce a single level of security to be applied for all participants. Hence, organizations with limited resources and technical means can participate – at least as Data Consumers. Still, the security level of these participants must be reliable and verifiable for other actors in the MDS ecosystem. Certain minimum-security requirements such as use of X.509 certificates issued by CySIMS for mutual Transport Layer Security, encrypted communication and use of unique certificate thumbprint for data access need to be met by all participants.

8.2 Certification Perspectives

Certification of participants and components is currently outside of the scope of the Maritime Data Space project. Still, we will cover the perspectives on certification in this section to show the framework and possibilities that IDSA offers to build additional trust and security into the Maritime Data Space as the ecosystem reaches a higher level of maturity.

Data security and data sovereignty are the fundamental value propositions of IDSA. Data sovereignty can be defined as a natural person's or legal entity's capability of being in full control of its data. Therefore, any actor in the ecosystem will be certified, including the core software components that the participants use to securely exchange data with one another. While the certification of organizations and individuals focuses on security and trust, the certification of components also refers to compliance with technical requirements ensuring interoperability. To ensure a consistent process in the certification of participants and core components, the IDSA uses a Certification Scheme comprising all processes, rules, and standards governing the certification process. The IDSA Certification Scheme follows best practices from other, internationally accredited certification concepts.

The certification process and roles are outlined in Figure 20 below. After a successfully completed evaluation process, the Certification Body awards an International Data Spaces certificate to the applicant. This certificate has a limited validity period. To renew a certificate before it expires, re-certification is required. The roles and responsibilities in this process can be defined as follows:

- **Certification Body:** The Certification Body oversees the certification process regarding quality assurance and framework governance. It defines standard evaluation procedures and supervises the actions of the Evaluation Facilities. A certificate is granted only if both the Evaluation Facility and the Certification Body have concluded that all preconditions for certification are fulfilled.
- **Evaluation Facility:** The Evaluation Facility is responsible for carrying out the detailed technical and/ or organizational evaluation work during a certification process. The Evaluation Facility issues an evaluation report for the respective organization/ individual or core component, listing details regarding the evaluation process as well as information regarding the confirmed security level.
- **Applicant:** The Applicant is the subject of the evaluation and certification process. An Applicant needs to actively apply to trigger the certification process. This applies to organizations or individuals that develop software components intended to be deployed within the International Data Spaces and to organizations that intend to become IDSA Participants.

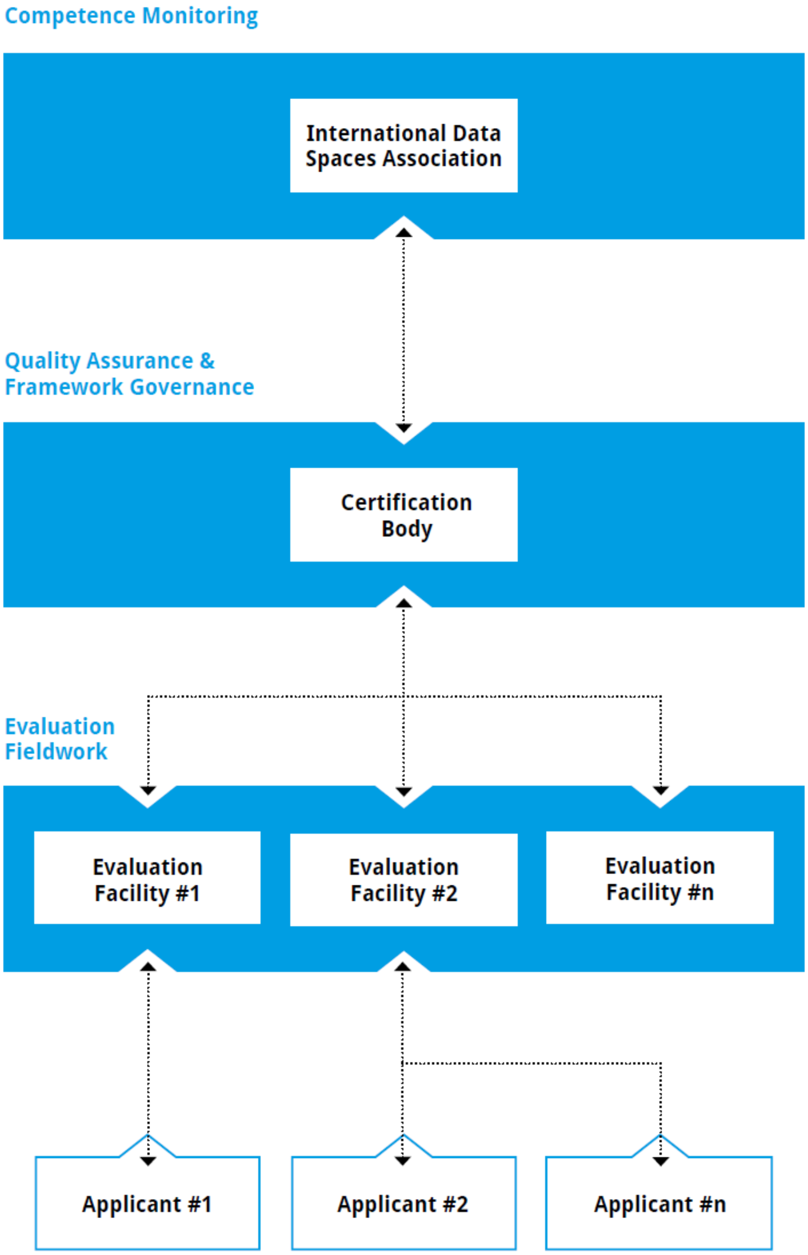


Figure 20 - IDSA Certification process

8.3 Governance Perspectives

The Governance Perspective of the Maritime Data Space follows the guidelines defined by the IDSA Reference Architecture Model, and defines the roles, functions, and processes from a governance and compliance point of view. The Governance Perspective defines the requirements to be met by the MDS ecosystem to achieve secure and reliable corporate interoperability between all actors and has been tailored to the maritime domain since the IDSA approach opens for customization of governance mechanisms for a specific domain and individual use cases.

The MDS ecosystem supports governance mechanisms by:

- Providing an infrastructure for data exchange, corporate interoperability, and the use of new, digital business models
- Establishing trustworthy relationships between Data Owners, Data Providers, and Data Consumers
- Facilitating negotiation of agreements and contracts
- Enabling transparency and traceability of data exchange and data use
- Ensuring that the data owner stays in control of data by implementing fine-grained access and authorization mechanisms
- Offering a decentralized architecture that does not require one centralized data platform provider

The following tables describe how the different roles and participants in the MDS ecosystem are related to governance activities. The overview also show which MDS technological components are involved at each level.

Data Owner and Data Provider	
Data Governance activities	• Define usage constraints for data resources • Describe the data source, publish metadata including usage constraints to Broker • Transfer data with usage constraints linked to data • Bill data (if required) • Manage data quality
Enabling and supporting MDS components	**Provider Connector** – allowing secure and encrypted exchange of data by use of X.509 certificates and mTLS technology. Allow and restrict access by use of unique certificate thumbprints.

Data Consumer	
Data Governance activities	• Use data in compliance with usage constraints • Search for existing datasets at the Broker Service Provider
Enabling and supporting MDS components	**Consumer Connector** – allowing secure and encrypted exchange of data by use of X.509 certificates and mTLS technology. Peer-to-peer concept with direct communication between connectors allows data provider to restrict access for each data consumer if usage constraints are violated. **Broker Service Provider component** – uses a metadata model that has been specified according to the Information Model developed by IDSA. The Broker provides a registration interface for Data Providers, and a query interface for Data Consumers.

Broker Service Provider	
Data Governance activities	• Match demand and supply of data • Provide Data Consumer with metadata
Enabling and supporting MDS components	**Broker Service Provider component** – uses a metadata model that has been specified according to the Information Model developed by IDSA. The Broker provides a registration interface for Data Providers, and a query interface for Data Consumers.