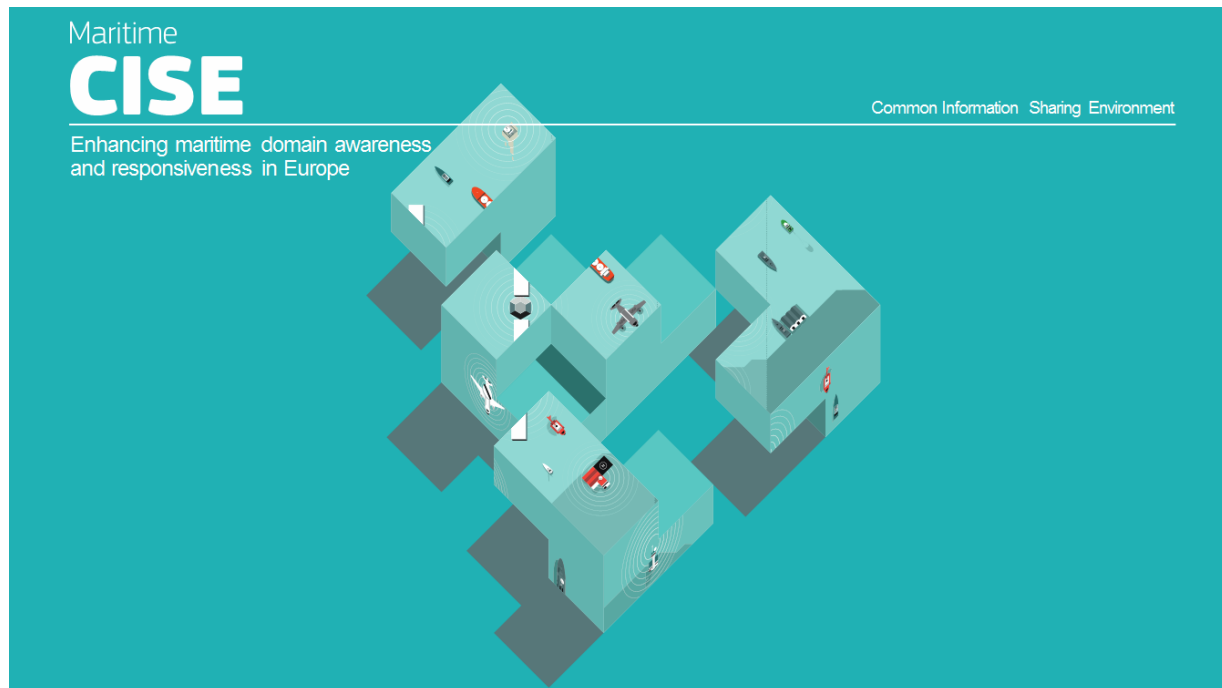


# ***CISE – the Common Information Sharing Environment for the Maritime Domain***



**EESC Safe Seas Conference  
Brussels, 24 March 2015  
T. Barbas, Joint Research Centre**

# JRC Maritime Affairs Unit - Activity areas

- **Maritime security** Maritime border control (EUROSUR), Piracy
- **Maritime transport** Oil pollution, Critical Maritime Routes
- **Fisheries** Common fisheries policy, Aquaculture, Illegal fishing (IUU)
- **Anti-fraud** Maritime containers monitoring for customs
- **Integrated maritime surveillance** Data exchange, interoperability
- **EU common tools** Copernicus (Earth Observation)
- **Multimodal transport safety** Air, maritime and rail
- **Common Security & Defence Policy** Maritime Capacity Building in Africa



**CISE is NOT a system.**

**It is a set of agreed specifications for data exchange between existing (legacy) systems in member states and agencies. The specifications are based on the results of CISE preparatory work with Member States.**



**CISE also includes some supporting tools:**

- **A common registry of authorities (i.e. contact details of CISE participants).**
- **A common registry of services (i.e. the menu of services provided by CISE participants)**
- **Virtual collaboration tools (e.g. instant messaging).**
- **...**

# The CISE principles



CISE must allow **interlinking any public authority in the EU** and in the EEA involved in maritime surveillance.

CISE must increase maritime awareness based on **need-to-know** and **responsibility-to-share** principles.

CISE must privilege a **decentralised** approach at EU-level.

CISE must allow interoperability among **civilian and military** information systems.

CISE must allow **interoperability** among information systems at the European, national, sectoral and regional level.

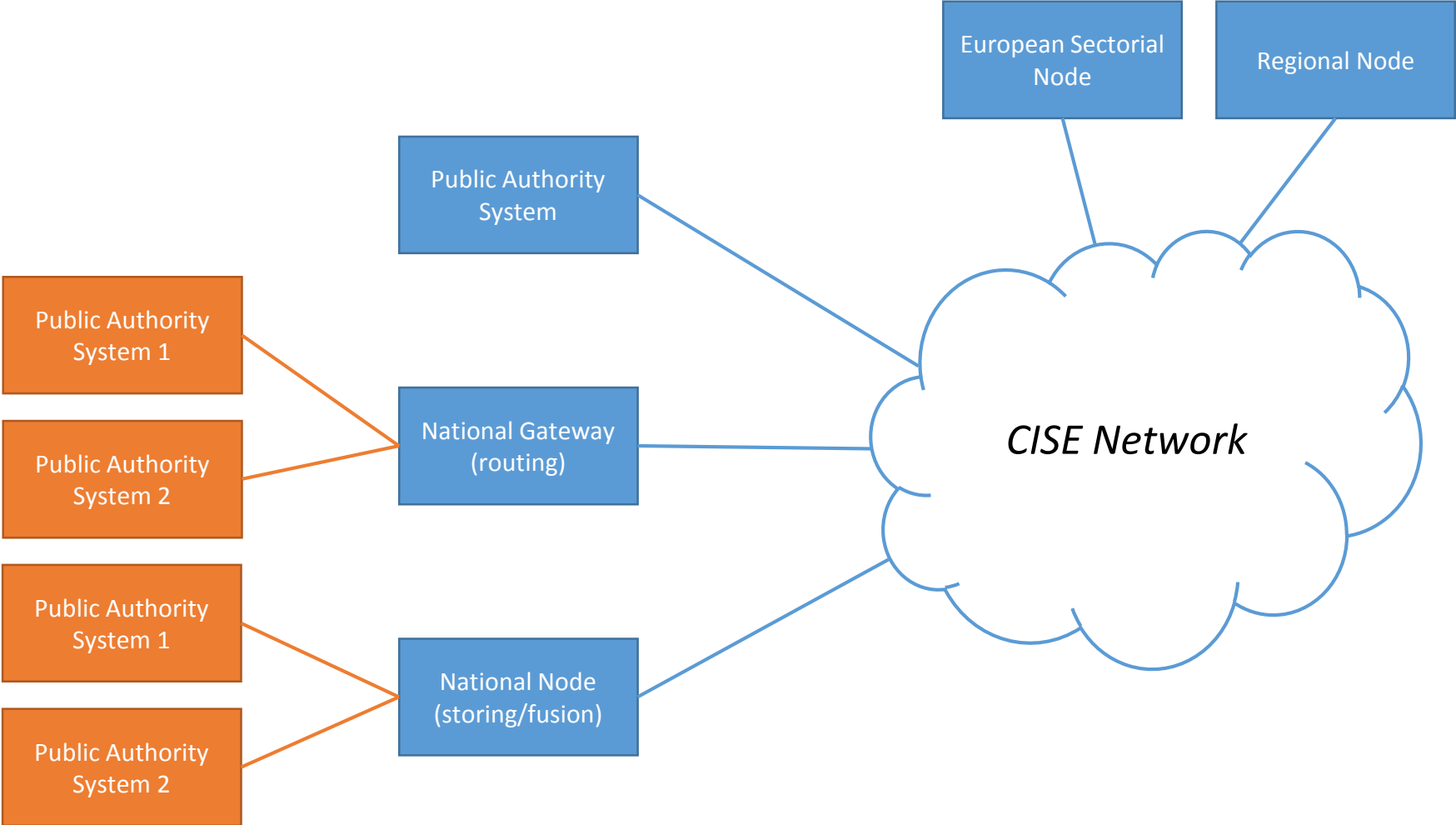
CISE must privilege **reuse** of **existing** tools, technologies and systems.

CISE must allow seamless and **secure exchanges** of any type **of information** relevant for maritime surveillance.

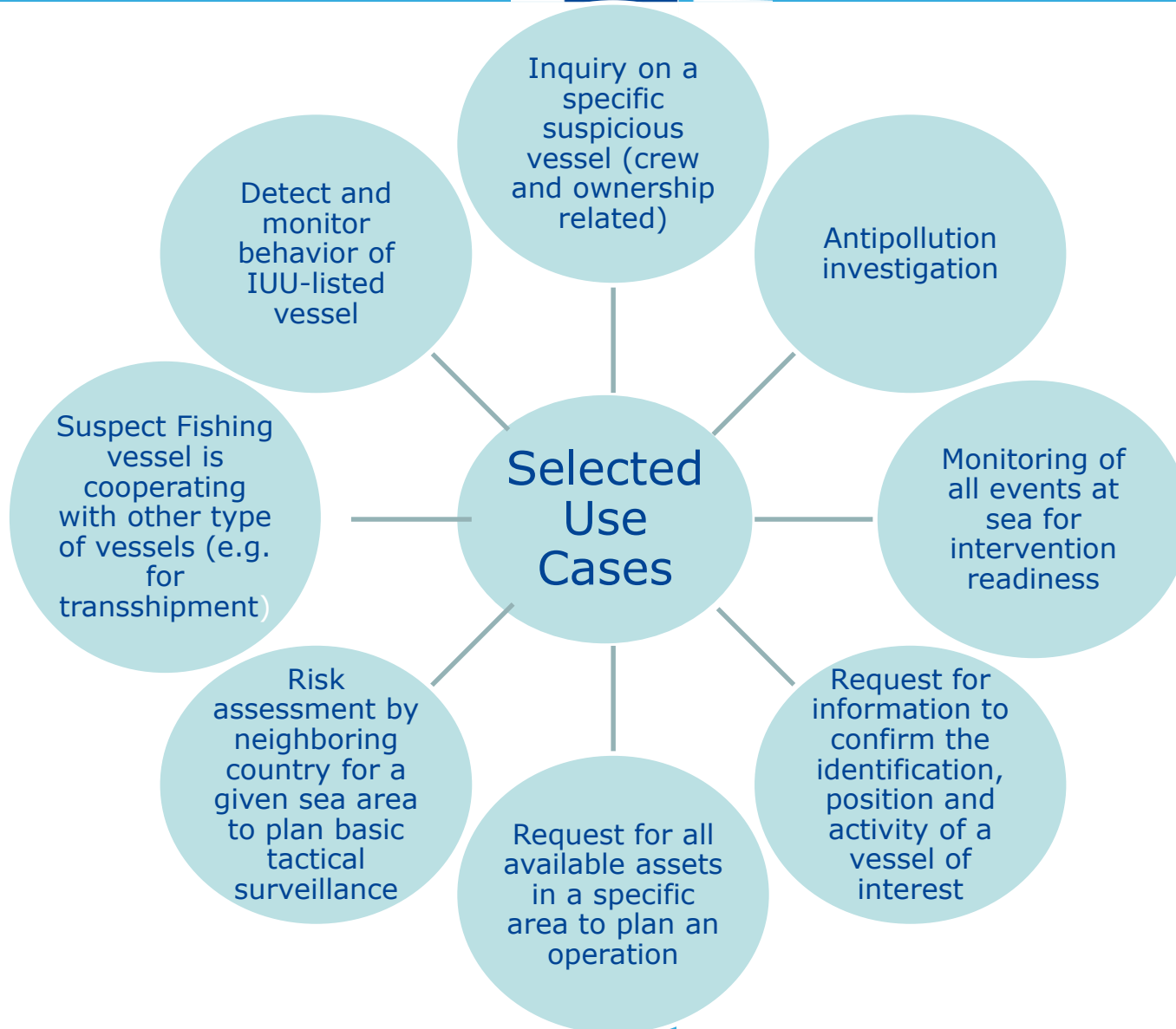
CISE must be **system neutral**.

CISE must make it possible for information providers to change their service offering.

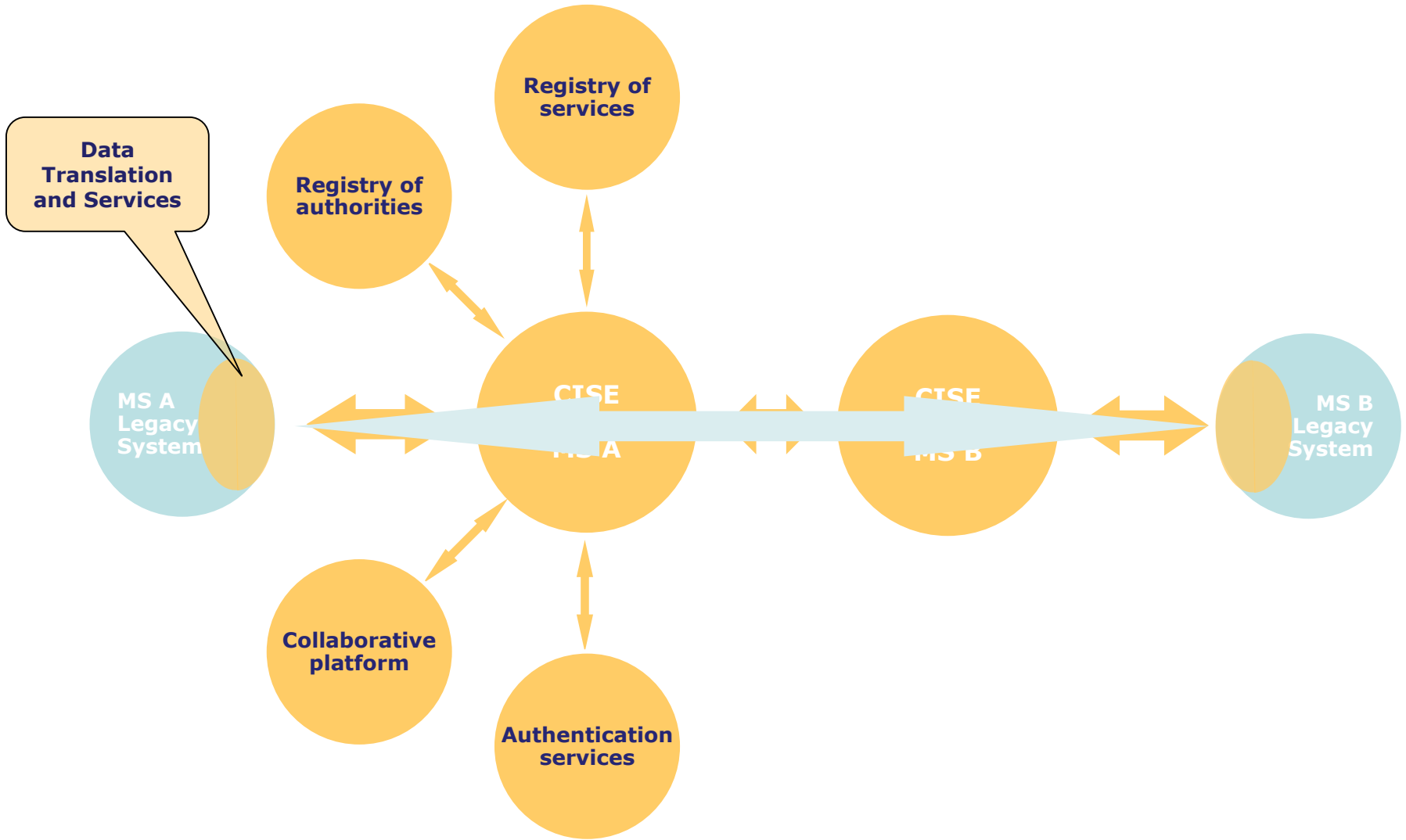
# The CISE Hybrid Architecture



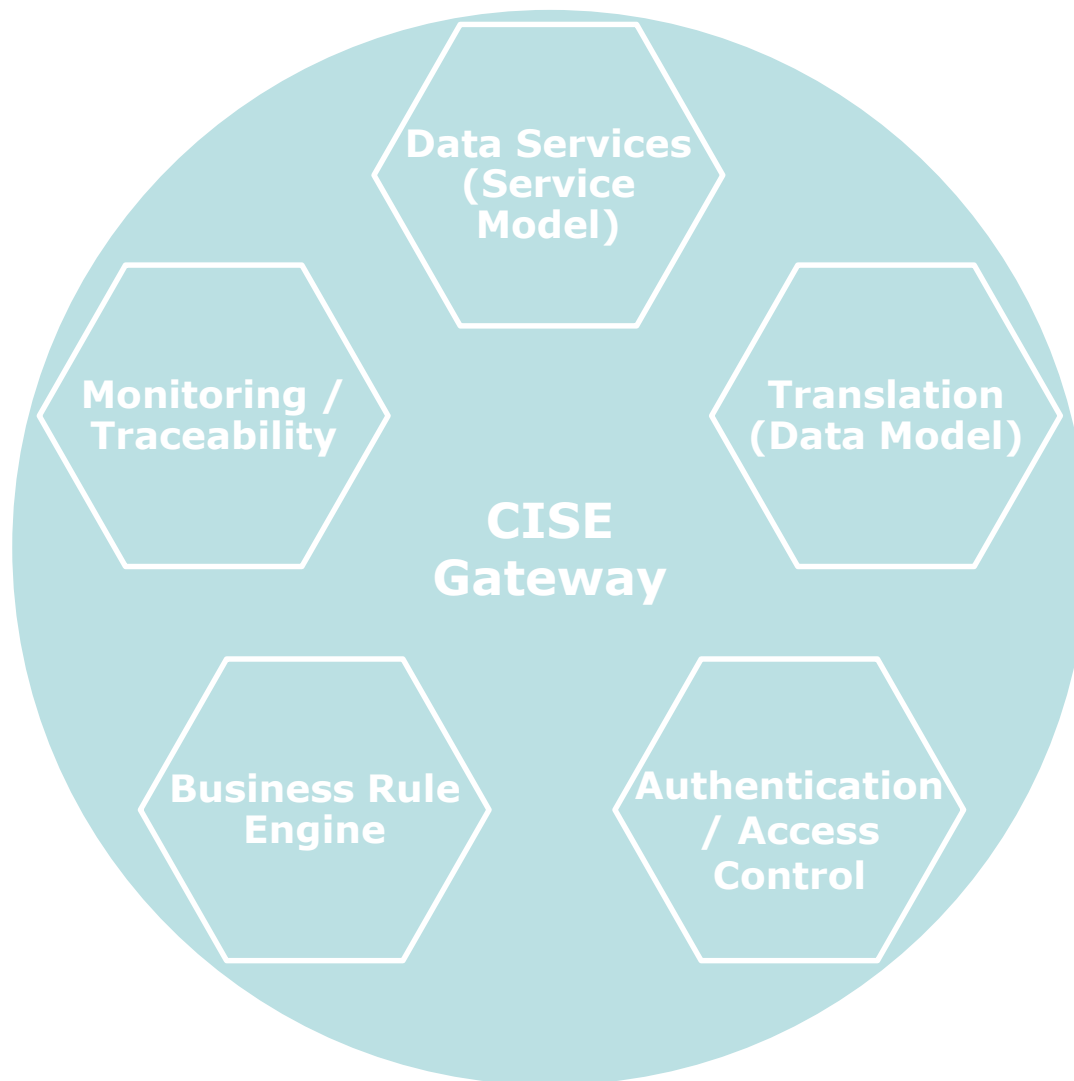
# Initial selection of CISE use cases



# CISE: the interfaces to build



# What is inside a CISE Gateway







## Relatively few technical obstacles expected

- Need to build the interfaces (many pieces will be provided centrally)
- Effort will be needed by the existing (legacy) systems to be able to integrate the additional information



## What is needed to tackle the non-technical obstacles

- Low initial investment to start at low cost
- Gradually building confidence and trust (e.g. through common projects, solid security and access rights, attention to personal data, regular communication with participants, sharing of experiences etc.)
- Focusing on business implementation after the technical part is over, with continuity and funding
- Investing in governance
- There is must be an advantage for participants from being in CISE



## **INSPIRE=Infrastructure for Spatial Information in EU**

- **For the purposes of Community Environmental policies**
- **INSPIRE needs: better information, better information flows, sharing of information, lack of standards, data not reusable...**
- **Started in 2001 as voluntary exercise, legislation in 2007**
- **Decentralized system, complex project aiming at long-term data interoperability, 250+ legally mandated organizations to develop the specs, implement infrastructures, 30+ spatial thematic areas (different communities, e.g. hydrography, transport, land use etc.)**



## SOME LESSONS

- **Not enough time to test the specs before making them a legal requirement**
- **Interoperability standards come with ambiguities and different flavors, not always plug-and-play**
- **Information exchange projects take time (2001...2007...2010 metadata ready, 2013 some data interoperable, ...2020 all data interoperable...)**
- **Voluntary approach also implies that the stakeholders who can invest will have greater influence on the outcome**
- **Some MS redesigned their internal data management processes**
- **Communication should be given high priority and continuity**
- **about existing community standards: build as much as possible on existing practices**
- **About sustainability: will need as much effort to maintain as to develop**



## **E-CUSTOMS=secure, integrated interoperable electronic customs (COM + MS)**

- Large set of systems based mostly on portals, with information entered manually (less on machine-to-machine)
- Secure network with leased lines, about 40 nodes (CCN-CSI)
- No central database (with few exceptions)

## **SOME LESSONS**

- Try to limit the operational overlap between available systems
- Building central components and interfaces is not enough; focusing on business implementation is necessary
- Governance needs to be planned and funded (e.g. collection of stats, monitoring, regular meetings, trainings, discussions, issues, strategy)
- Identify the remaining legal obstacles as early as possible
- Machine-to-machine pays: upfront investment higher, need to dispel fear of automation, but operational costs will be lower
- Use the frontrunners and their success stories to entice others



- An initial set of security requirements exists already
- A detailed threat and risk analysis study is yet to be done
- CISE relies on the security of existing systems: hardening the security of legacy systems against attacks is necessary
- Hardening the security of CISE Gateways is already planned

## Other:

- Monitoring the data flows through the CISE Gateways will help early detection of cyberattacks
- In CISE you can share data, but you cannot modify it
- CISE is a decentralized system and the risk is distributed
- The CISE network gives rise to many sources of information and allows for wider cross-checks
- It should be possible to qualify the security level of each CISE participant in advance – and deny some connections
- Information flows if access rights OK and security of the connection OK



- There is a need for resources (technical skills and budget)
- Funds can be used to migrate legacy systems to state-of-the-art architectures (SOA, web services etc.) to enable them to exchange information (e.g. DG MARE call for proposals for interoperability improvements).

## But

- Most IT systems undergo evolutive maintenance anyway
- If national systems are coherent with each other, it will also be also easier to share information
- Some MS will take the opportunity to completely redesign their data management processes

**Costs and benefits should be measured (e.g. through MS reporting)**

# Joint Research Centre (JRC)

<https://ec.europa.eu/jrc/>

Contact:  
thomas.barbas@ec.europa.eu

*Serving society*  
*Stimulating innovation*  
*Supporting legislation*

