



Panel Discussion:
NEW IPCEI-CIS REFERENCE ARCHITECTURE

NexusForum 2025, November 6th

Matthias Kuom

DLR-PT



IPCEI-CIS is the Next Generation Cloud Infrastructure and Services project, involving 12 EU member states and around 120 industry and research partners.



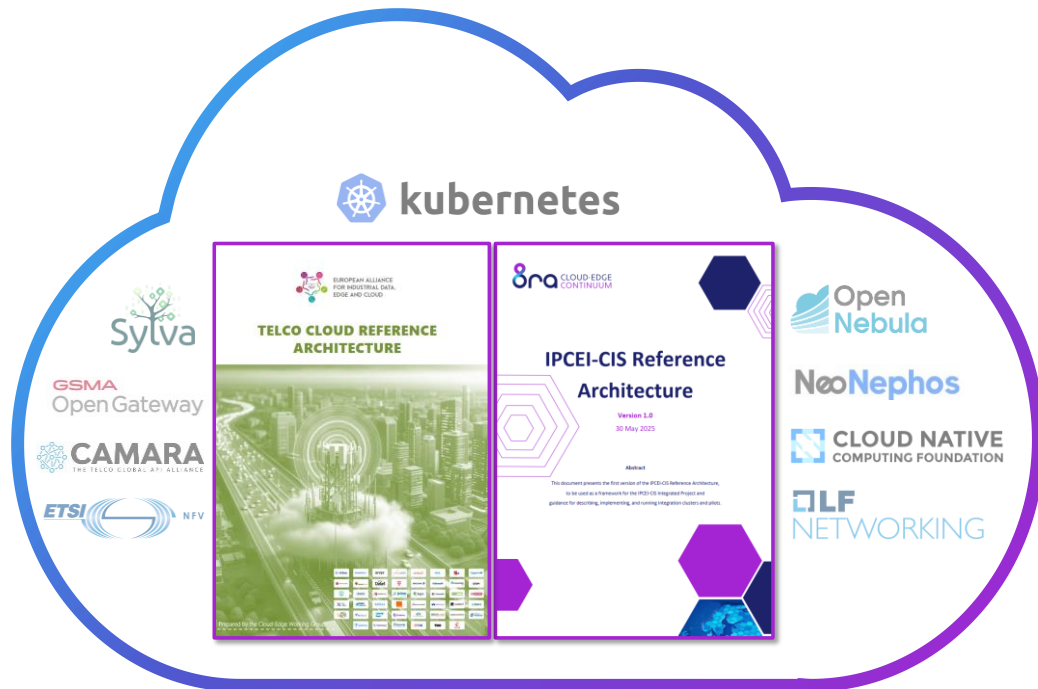
8ra aligns the IPCEI-CIS projects, creates a framework for future continuation and extension beyond the IPCEI-CIS duration.



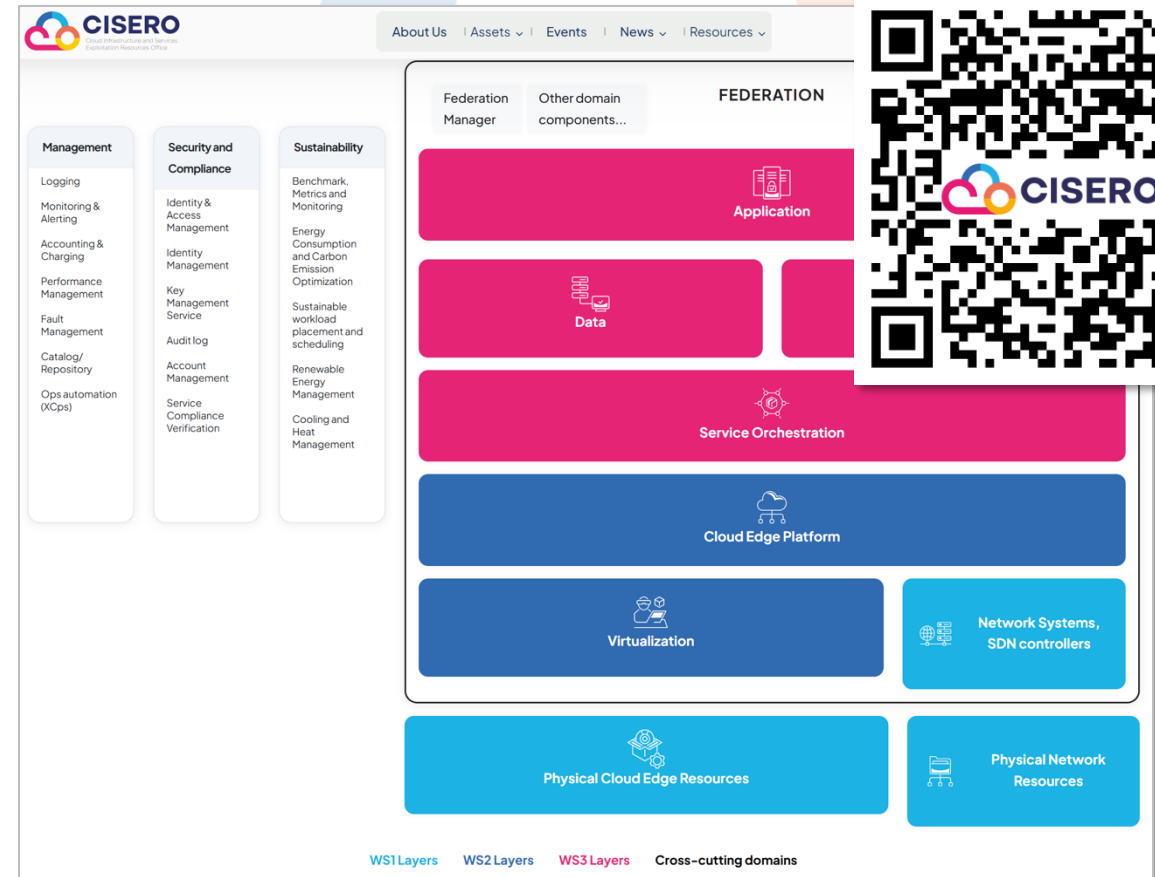
CISERO facilitates the adoption and exploration of IPCEI-CIS results, enhances collaboration and fosters a strong community of practice.



Alignment of the IPCEI-CIS Reference Architecture with the Telco Cloud Reference Architecture of the **European Alliance for Industrial Data, Edge and Cloud**



IPCEI-CIS Reference Architecture | CISERO



Submit your feedback >

Andreas Schlosser
*BTP Cross
Projects, SAP*



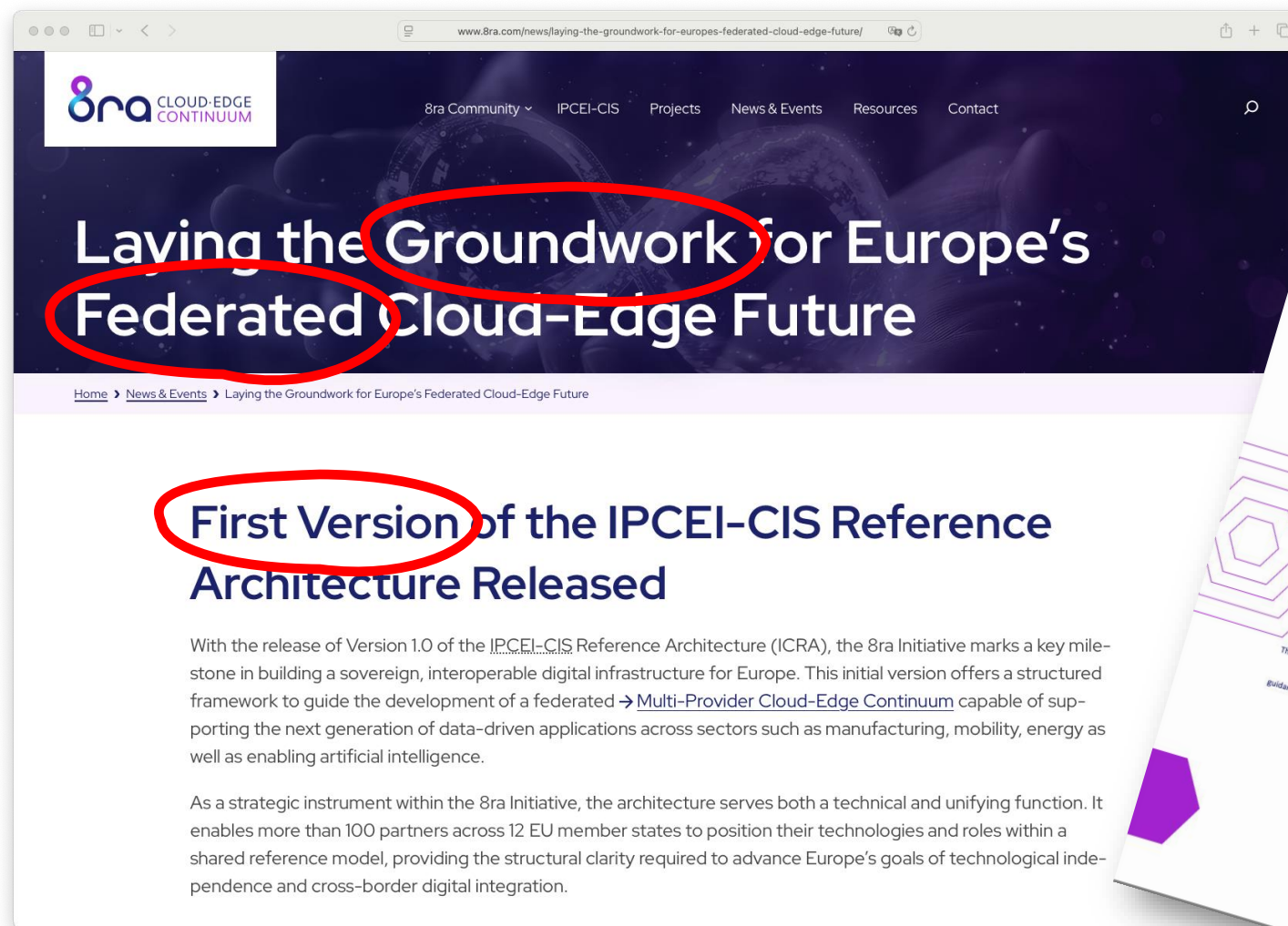
Mauro Renato Boldi
*European Project
Manager, TIM*



Pawel Maslowski
*Chief Innovation
Officer, Oktawave*



Published in May 2025



Architecture Task Force

The IPCEI-CIS Reference Architecture document is produced by the **Architecture Task Force**.

This task force includes representatives from the IPCEI-CIS workstreams:

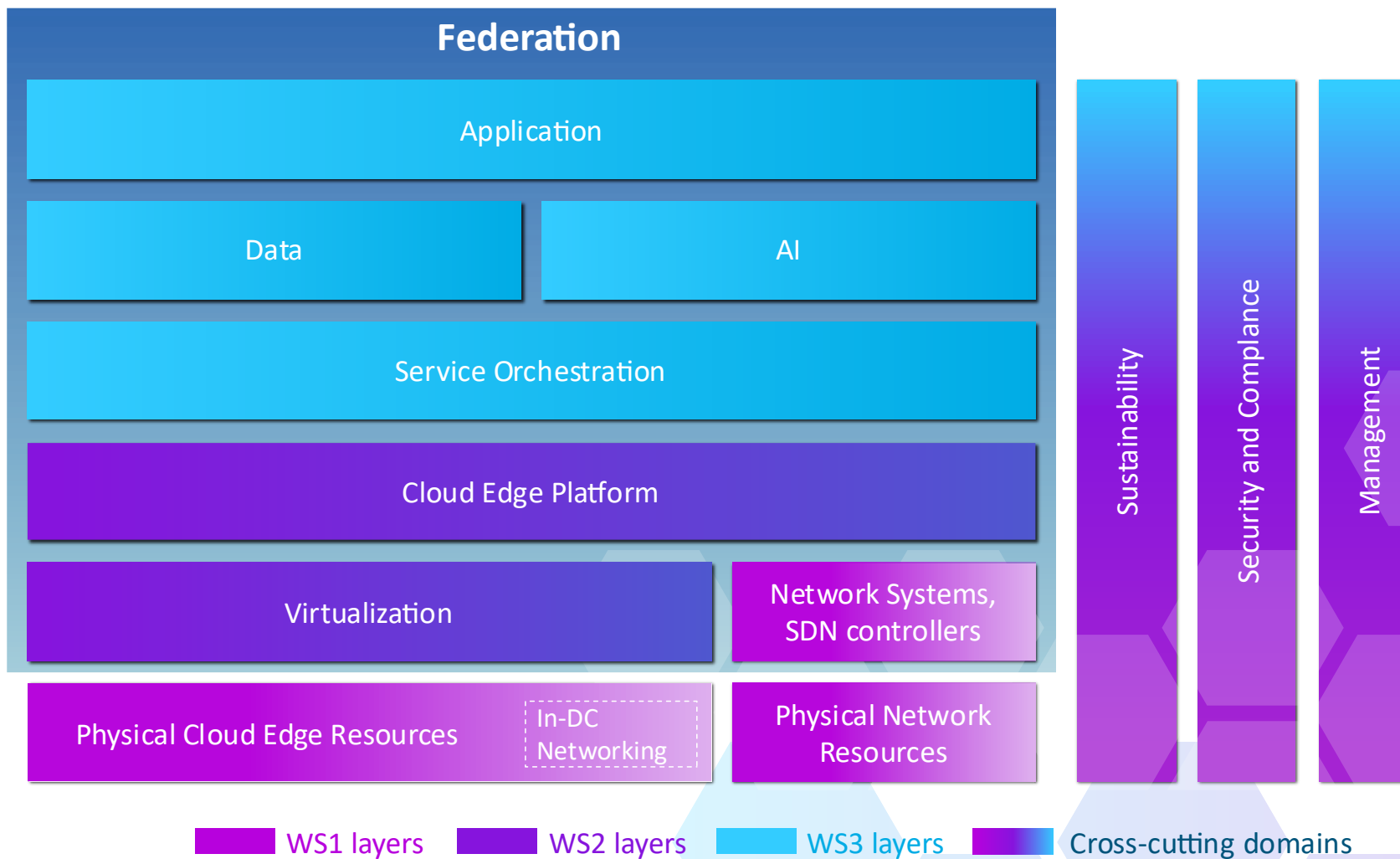
- Workstream 1: **Cloud Edge Continuum Infrastructure**
- Workstream 2: **Cloud Edge Capabilities**
- Workstream 3: **Advanced Smart Data Processing Tools and Services**
- Workstream 4: **Advanced Applications**
- Cross-workstream **Security**
- Cross-workstream **Sustainability**

Layers & Domains

The Reference Architecture document describes layers and domains.

- **Layers:** Levels of abstraction.
From application layer to physical hardware.
- **Domains:** Cross-cutting aspects.
Security, federation, sustainability, and management.

High Level Overview



Groundwork

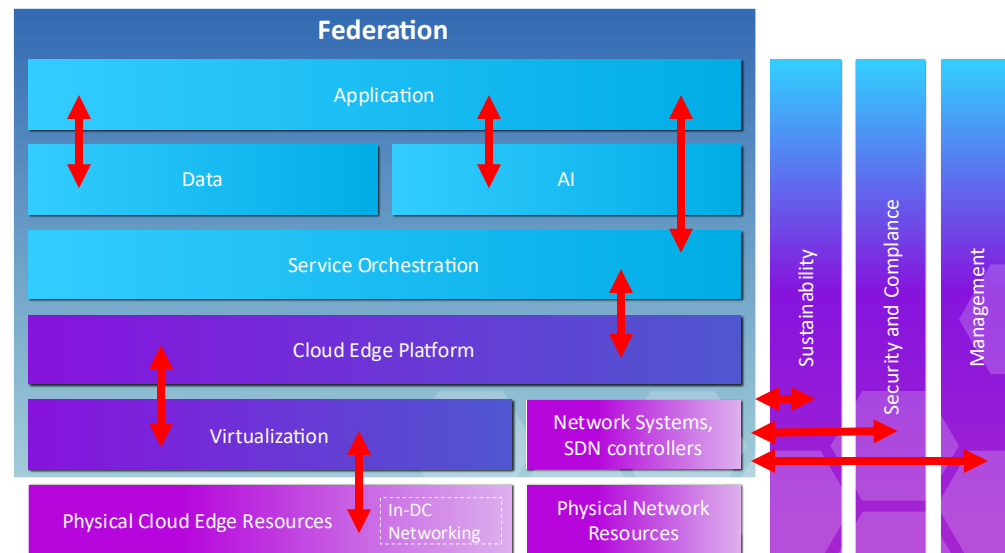
There is **nothing too surprising**.

Version 1 of the ICRA provides the **necessary groundwork**:
it defines building blocks and terminology for further discussions.

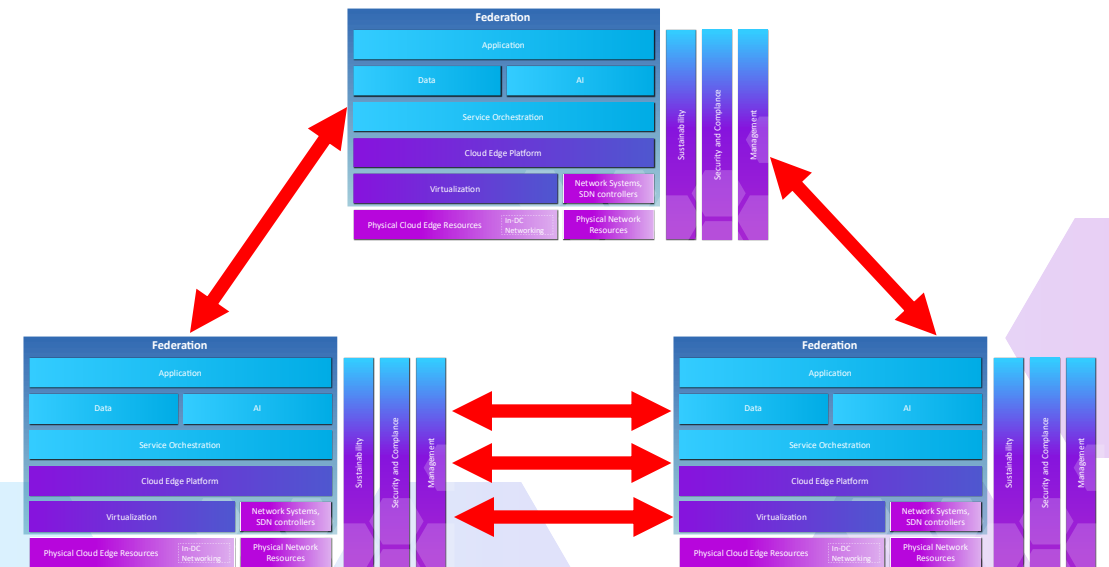
Federation and partial **standardization** throughout the cloud-edge continuum across most layers will be a significant innovation. This initial version of the reference architecture only hints at this potential.

Outlook: Version 2

- The Architecture Task Force is working on **ICRA version 2**.
- The release is planned for the **end of 2025**.
- There are two focus topics: **functional interfaces** and **federation**.



Functional Interfaces

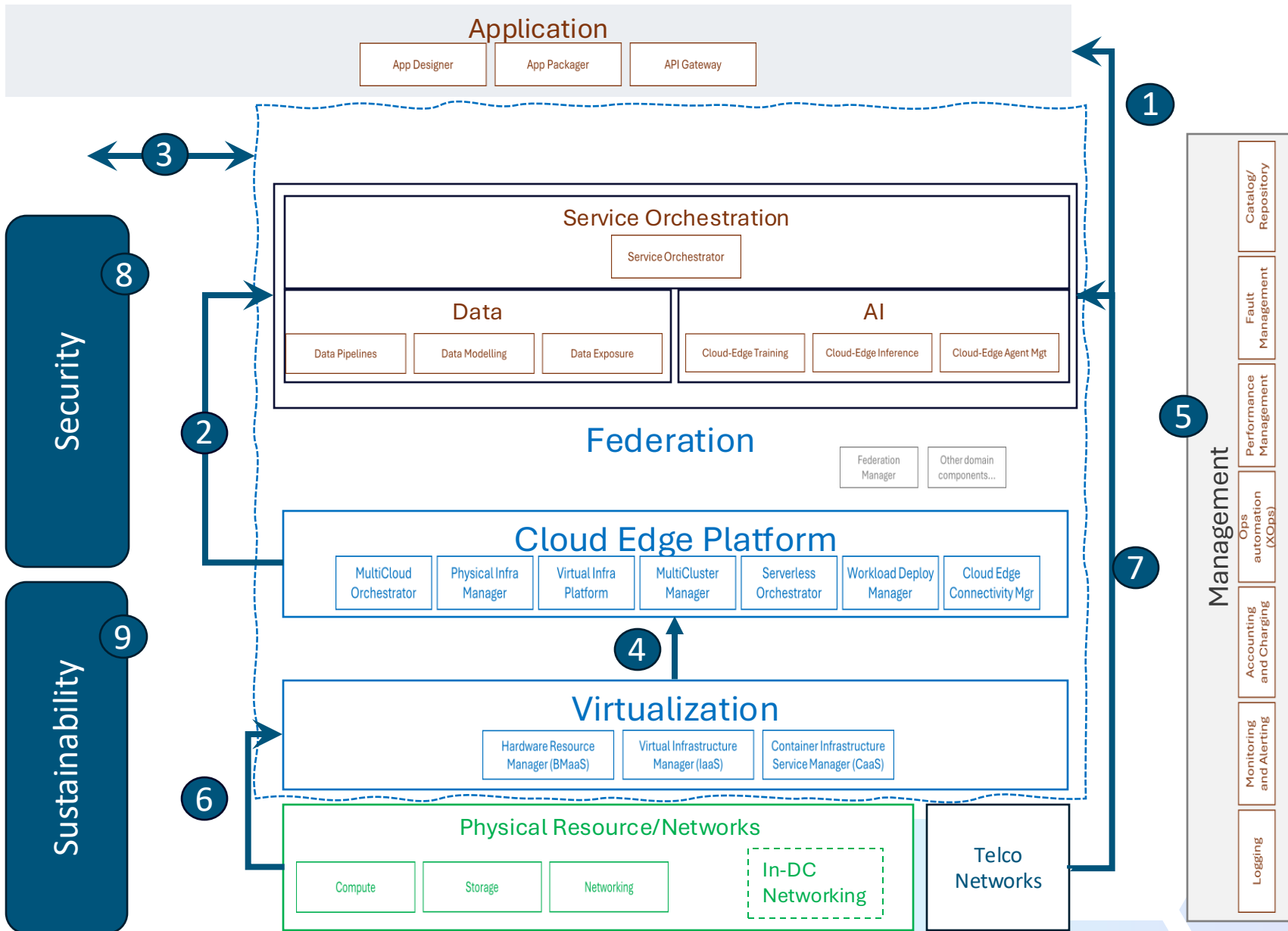


Federation

Functional Interfaces

- Functional interfaces are the **connection points** between different layers and domains.
- The Architecture Task Force **collects standards, APIs, and de-facto standards** defined by open source projects from 8ra participants.
- The ICRA version 2 will include **a report and some recommendations**. These will be refined in future versions.



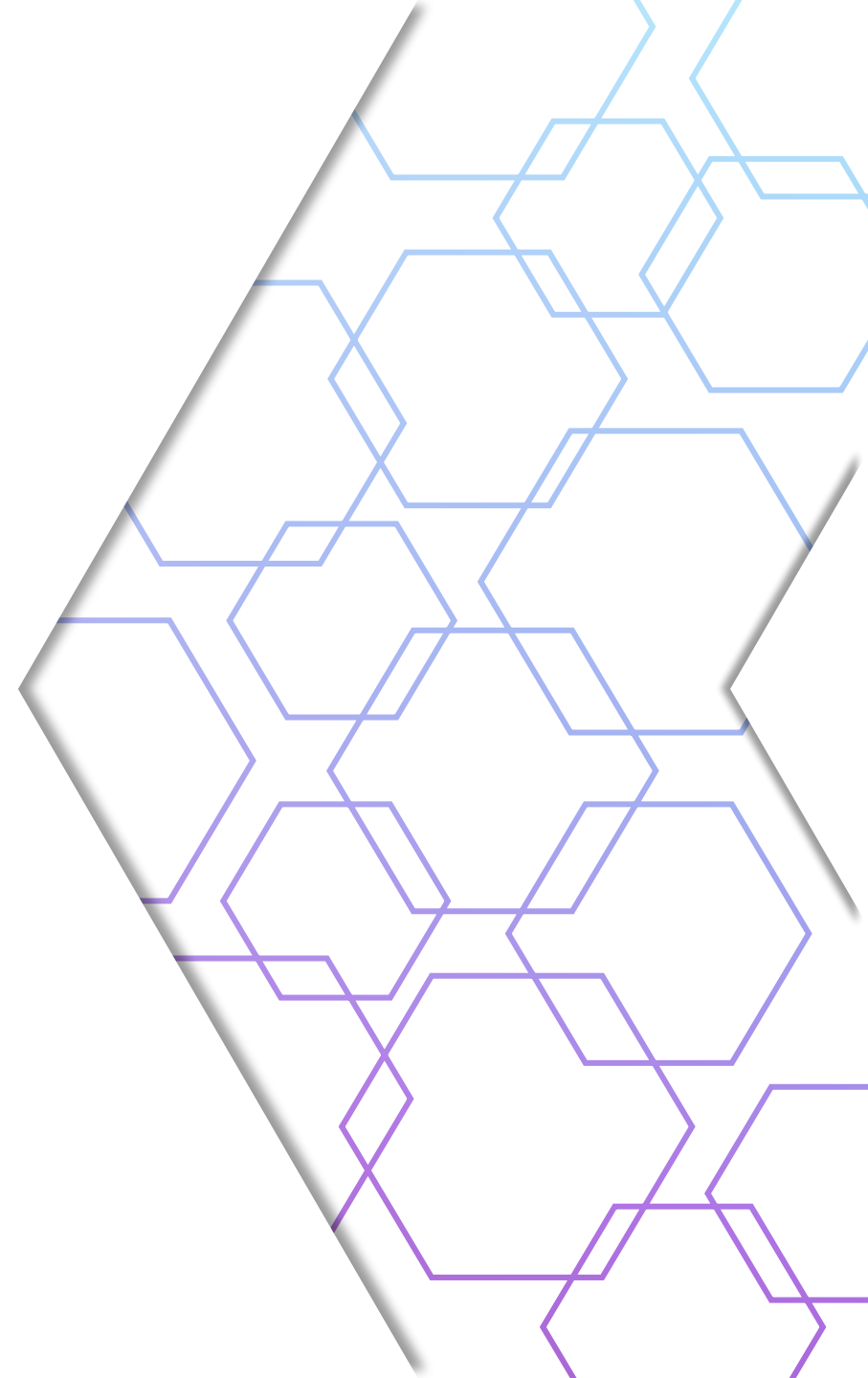


FUNCTIONAL INTERFACES

- ① SO Layer-App Layer
- ② Platform-SO Layer
- ③ Federation
- ④ Virt Layer-Platform
- ⑤ Mngmt-Platform
- ⑥ Phy Resource-Virt Layer
- ⑦ SO-Telco networks
- ⑧ Security
- ⑨ Sustainability

Federation

- Discovery, connection, and interoperability in a **Multi-Provider Cloud Edge Continuum**.
- The Architecture Task Force is currently discussing whether we can find a **common language to describe resources, services, and dependencies** in a multi-provider setup.
- ICRA version 2 will contain **only a few aspects of federation**. Future versions will provide more details.



Security

Key Points

Establishes a **unified security framework** across IPCEI-CIS partners

Standardizes **security components, APIs, and compliance practices**

Ensures **interoperability** across a European multi-cloud & edge ecosystem

Builds a **baseline security posture** aligned with EU standards (NIS2, CRA, EUCS, EUCC, GDPR)

Delivers a **shared integration language** and API blueprint for seamless security services

Provides **testbed environment** for validation & cross-partner alignment

Core Activities

Classification of security building blocks across layers & domains

Detailed technical & functional documentation of partner security modules

Identification of **gaps and overlaps** across solutions

Joint development of **mitigation & enhancement strategies**

Continuous **threat analysis and compliance alignment**

Security Domains Covered

Identity & Access Management

Network & Data Security

Application & Device Security

Security Operations & Monitoring

Governance, Risk & Compliance

Resilience & Availability

Privacy & User Control

Future Threat Preparedness (AI-based attacks, quantum threats, satellite & mesh security)

Strategic Value

Builds **European digital sovereignty** through secure cloud-edge federation

Enhances **cyber resilience & innovation** across EU partners

Enables **secure cross-border services** and infrastructure collaboration

Positions project for **long-term regulatory compliance & emerging threat readiness**



Thank you!



www.8ra.com