Project Description

Important Project of Common European Interest on Compute Infrastructure Continuum (IPCEI-CIC)

Please note this document reflects the current stage of deliberation among the participating member states and is subject to changes and improvement. It is intended to be used in the national procedures such as call for proposals or calls of expression of interest.

Version	Date
1.2	30 September 2025
1.3	02 October 2025

Table

1. Political Rationale

1.1 Artificial intelligence capacities as basis for economic growth and gain competitiveness

The European Union as a unique digital single market is challenged by the rapid digital developments. The European Union faces a twin challenge: to increase the adoption of key digital technologies in its economy to improve its competitiveness, and to do so in a way that strengthens its technological sovereignty and the resilience of its infrastructure and societies. The engine of the next industrial revolution will be artificial intelligence (AI) which is the major paradigm shift and the technological foundation for the development and use of digital solutions today and tomorrow. A fundamental prerequisite to meet these requirements are the integration of vast types of infrastructures, such as cloud and edge. Europe´s industry needs access to the latest software, AI models, hardware, as well as high-end computing resources. Examples of innovative AI solutions includes autonomous production, AI-driven robotics, AI-supported product design and Industrial Metaverse applications in the industrial sector. Another example is the automation and optimization of network management in the telco sector.

Therefore, it is necessary that European industries have equal access to sufficient computing and data resource for AI while reducing their dependence on non-European solutions and providers. For European industries to have the sovereign choice of increasing resilience as well as security, they need to rely on a combination of new and existing European technologies through increased interoperability.

In this context, the European Commission has introduced the AI Continent Action Plan, which is a comprehensive strategy to position Europe as a global leader in artificial intelligence. The first pillar of the plan is the investment in computing infrastructures, allowing innovators and researchers to train and finetune AI frontier models, notably through AI-Factories and Gigafactories. Complementary to this, the EU Cloud and AI Development Act (under development) will aim to triple the EU's data centre capacity within the next five to seven years. Another key pillar is the Apply AI Strategy, intended to accelerate AI adoption and drive innovation through AI solutions "made in Europe".

A comprehensive and integrated Important Project of common European Interest (IPCEI) will leverage and accelerate those activities. Driven by Member States, it will ensure the integration of the different national requirements and the bundling of competences on a European scale. Last year, within the Joint-European-Forum (JEF) 19 Member States discussed and identified possible key digital technologies feasible under the IPCEI-Communication of the EU Commission. A group of 13 Member States endorsed in November 2024 the two digital IPCEI proposals (IPCEI AI and IPCEI CIC) addressing the following challenges.

1.2 EU Challenges for infrastructure for AI

Global developments in AI are accelerating fast, injecting a sense of urgency: the European Union must foster an environment in which computing, interconnectivity, cloud, AI and software providers can grow and provide AI capacities and services to industries, academia, public sector and citizens. This should be achieved along a distributed computing and software stack, from bare metal solutions to specialised AI services. In this context, the EU need to address the following challenges:

(1) Low adoption rate of AI solutions due to limited infrastructure capabilities:

Access to computing capacities, together with the availability of high-quality data is the backbone of AI. EU suffers from low adoption rate of AI technologies in industries, due to high ramp-up cost and lack of "plug and play solutions". Additionally, there is a lack of certified trust for AI solutions. Today, most AI solutions are locked in proprietary infrastructures. This leads to a limited availability of capacity for AI solutions.

In addition, Europe lacks the sufficient infrastructure, specialized to the need for AI to address its future needs. Currently, it is estimated that 70% of worldwide AI compute capacity is deployed in the United States with Europe accounting only for a 4% of it. Moreover, European industrial electricity costs[1] are between 1.5 and 3 times higher[2], limiting the competitiveness of European players in the field.

(2) High fragmentation of the EU cloud market as well as the lack of state-of-the-art AI and cloud technologies:

The development of state-of-the-art AI solutions in the EU requires significant investments, in R&D and first industrial development. AI development is fragmented and uncoordinated across academic, public, and private players. One essential prerequisite for AI development and operation is the access to cloud infrastructure. Due to the high fragmentation of the European cloud market, European cloud providers are not able to meet the necessary demand for AI training, fine-tuning, and inference resulting in a lack of state-of-the-art AI. The existence of a sovereign European infrastructure remains an unanswered challenge. Overcoming this challenge provides highly flexible interconnectivity, access to data, better competitiveness of individual providers, and of the whole European economy[3].

(3) Lack of interoperability and connectivity among European computing capacities:

The integration and the interconnection between different computing resources across different European regions and between cloud and edge fragmented infrastructures is complex and cost intensive. Future computing resources need to be integrated seamlessly to meet the high requirements of AI powered applications in terms of e.g. latency, bandwidth, security, reliability or energy efficiency. This level of interoperability and the necessary connectivity infrastructure is a prerequisite for future use cases, e.g. real-time data processing (drones, autonomous trains/ trucks/ cars, smart factories) and is of a highly strategic value for the EU.

(4) Insufficient readiness for future AI developments:

Due to the current lack of the European providers to meet the requirements of next generation AI solutions, there is a risk of not keeping pace with the rapid global AI development. For certain future AI related use cases, Europe lacks the sufficient capacity to train and run AI solutions on location where the data is generated and stored. Therefore, a federated distributed ecosystem needs an intelligent orchestration of distributed computing and connectivity functions allowing for secure and confidential transfer and processing of mass data. This systemic approach is not limited to the infrastructure including storage, network and compute capabilities but also considers software stacks and support services.

An important success factor in supporting the resilience of the EU is to achieve technological sovereignty by ensuring that AI foundation models and the necessary supporting services are offered by European providers. This implies developing a common infrastructural ecosystem for AI, by making compute resources available and optimizing the hardware and software stacks.

Finally, the EU's objectives for the digital transition as well as strategic sovereignty shall foster the deployment of AI capacities and capabilities. The aim is to strengthen the development of the sovereign digital value chain and its resilience, from data center operators to AI service providers.

[1] EUR-Lex - 52025DC0072 - EN - EUR-Lex

[2] https://geopolitique.eu/en/2025/02/10/financing-infrastructure-for-a-competitive-european-ai/

[3] https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en

2. General Objectives and Scoping of the IPCEI-CIC

To comply with the IPCEI communication of the EU Commission, the two proposed IPCEIs (IPCEI AI and IPCEI CIC) as State aid instruments shall be designed in two distinct ways: the first with the focus on R&D&I and the second focusing on deployment of infrastructure. The shared objectives of the IPCEI on research on Artificial Intelligence (IPCEI-AI) and the IPCEI on deploying compute infrastructure (IPCEI-CIC) is to boost Europe's competitiveness in the global digital economy by fostering innovation and investment in developing AI capabilities and facilitating the access of European companies of all sizes to AI technologies and services. EU stakeholders (whether AI users or developers) deserve a resilient and secure environment consisting of hardware as well as software capabilities. The IPCEIs will enable all Member States to follow up on their respective AI strategies and collectively equip the EU to develop a next-generation European AI ecosystem that meets the needs of European stakeholders. The IPCEIs shall allow a better coordination across providers, companies, academia and countries to avoid duplication of work and inefficiencies in AI research and development. The IPCEIs should be able to complement the existing developments by IPCEI-CIS, as part of the 8ra-Initiative. They shall adhere to strict ethical guidelines and regulations, such as GDPR, DGA, Cybersecurity Act and AI Act. In addition, they could benefit from the developments fostered by projects in HORIZON EUROPE under the 3C's (Connected Collaborative Computing Networks), which aim to develop an open and sovereign platform and an ecosystem of users on different verticals around the telco-edge-cloud convergence.

For the European Union, criteria to improve technological and digital sovereignty are of the essence. Therefore, the establishment of a European wide ecosystem which ensures users/consumers and businesses to choose their competent service providers independently and to prevent vendor lock-ins for compute and data (incl. AI and cloud) services is necessary. In this ecosystem, data shall be processed and transferred according to the users' preferences regarding the scope, duration, subject matter, conditions, and partners of the exchange. Also, data shall be processed and transferred under the latest security and resiliency standards and according to the applicable EU regulations.

The purpose of this project description is to support the scoping of the IPCEI-CIC. Furthermore, it shall be implemented by the participating Member States in the forthcoming competitive, transparent, and non-discriminatory procedures for the selection of eligible partners for the IPCEI-CIC.

The objective of the IPCEI-CIC is to develop a sovereign computing infrastructure in Europe, provided by a multi-provider architecture, not limited to but focusing on the deployment of AI solutions. To ensure broad economic benefits, the supported projects should contribute directly to the development of the European digital value chain – from the construction of data centers to the provision of cloud services. The ability to train and run AI solutions at the location where the data is generated is important. It is a systemic approach to a federated distributed ecosystem with intelligent orchestration of distributed computing and connectivity functions allowing for secure and confidential transfer and processing of mass data. The project should focus on:

1.) Infrastructure deployment:

- Deployment of a scalable Infrastructure-as-a-Service (IaaS), which is highly agile consisting of cloud and edge platforms on a European scale to meet current and expected future demand.
- Regional deployment of infrastructure as part of a sovereign EU-wide network. This network should be interoperable and accessible through open and non-discriminatory access, pricing, and network operation to all interested parties
- Deployment of state-of-the-art European cloud and AI energy efficiency technologies, to best meet the innovation criteria, particularly with regard to the environmental footprint.

- Deployment of competitive European cloud and AI services. This way, all European industries can benefit from state-of-the-art cloud and AI infrastructure and associated cross-border services.

2.) Federation and connection in a network of sovereign EU-wide cross-border interconnected infrastructures that act as a compute continuum:

- Creation of a federated, distributed ecosystem of infrastructures on a European scale operated on common rules and conventions.
- Integration in a common architecture framework: The sovereign infrastructure should be deployed using IPCEI-CIS technologies (or equivalent technologies) to provide seamless operations, e.g. to leverage the development and training of AI models.
- Ensuring interoperability to allow multiple entries (from edge to cloud), applying a continuum concept for the purpose of the analysis, processing, storage, and data generation capabilities.
- Generation of blueprints of functional infrastructure.
- Focus on secure and energy efficient compute technologies.
- Ensuring multipurpose capabilities able to operate mission critical uses cases , not limited to AI.

3. Application Scenarios

The following application scenario descriptions do not represent a fixed or exhaustive list of project scopes in the IPCEI. They rather serve as illustrative examples of areas which could be addressed by project proposals.

3.1. Exemplary application scenario #1: Near-premises infrastructure, operated by a telco edge provider

Near-premises infrastructures, such as telco edge nodes, are distributed computing nodes that are directly integrated into telecommunications operators' networks. They provide compute capacity for third-party applications and enable ultra-low latencies for optimized connectivity. This connectivity provides a direct link between data generators-consumers and users over the mobile networks of the provider. It enables devices and services via sim card with 5G and edge. This could enable new use cases with requirements for:

- Low latency (plus jitter, etc.)
- Connectivity reliability
- Security, data privacy, and data sovereignty stemming from near-on-prem location, potentially with dedicated routing/slices

Near-premises infrastructures enable new services that combine network services with distributed, close to the data-generator and consumer computing capacity: (1) optimized traffic routing, selecting the best route and the nearest edge location for each user to reduce latency, data privacy risks (due to reduced data flows), and network traffic; (2) customized data traffic paths, to ensure that data only travels through allowed areas and networks; (3) network Quality-of-Service (QoS) on demand; (4) enhanced mobility for users thanks to the distributed presence of telco edge nodes and connectivity. Infrastructure capacities for near-premise, such as telco edge has this exemplary configuration:

- Computing servers with AI accelerators including GPUs for processing AI workloads
- Network integration between different network providers to be able to reach multiple nodes in the different countries over the mobile networks (5G, fiber) of each operator

- Networking components co-located with the computing servers such as UPFs, Security Gateways
- Datacenter facilities with appropriate security, cooling, power availability, high bandwidth, and high availability connectivity
- Software required to orchestrate the infrastructure including managing the full lifecycle of edge applications, configuring and optimizing the networking routes, etc.

Currently, there is limited availability of near-premise, installed capacity across Europe capable of delivering next-generation, latency sensitive digital services. The main reasons why this has not been deployed are:

- **Standardization and harmonization gaps**: Huge value for industry and EU customers/users come with EU interoperability and a cross-country and cross-operator solution ("cloud roaming"), which enable standards and solutions regardless of the users' home-country and allow a seamless handover between countries for EU-wide use cases.
- **Lack of technology maturity:**
    - In general, the market maturity for telco edge services has not yet emerged. Although the potential usage scenarios are already existing in the industries.
    - This is further compounded by the lack of available commercial offerings, which discourages experimentation and development. As a result, a self-sustaining ecosystem has not yet emerged.
- **High upfront investment**: Deploying edge nodes at scale requires significant capital for decentralized capacities. This imposes a high competitive risk for early movers.

3.2. Exemplary application scenario #2: Satellites for AI-Factories or AI-Gigafactories

Satellites for AI are distributed cloud infrastructures that supplement large, centralized data centers by offering training, fine-tuning, and inference services for smaller or specialized models. Positioned at various scales as regional AI hubs they address the demand outside of LLMs or LRMs while staying accessible to organizations of different sizes.

These satellites are part of the cloud and AI service ecosystem providing services required for the AI value chain. As those, they typically complement the services of AI-Factories and AI-Gigafactories with which they are linked in terms of interoperability. While the satellite might focus on services such as pre-processing and curating of data under privacy requirements, the AI-Factories will provide on-demand access capacity and training of large volumes of non-private data, which is shared by collaboration organizations. Typically, the linkage will be implemented by means of standardized API's.

Unlike large AI-Factories that prioritize frontier-size models, AI satellites can concentrate on specific industries and use cases. Customers in certain industries may have specialized computational or data-handling requirements that a satellite is uniquely positioned to fulfill. These satellites might also provide regional coverage e.g., for industrial regions. Through the development of implementation-blueprints (based on first implementations) effective rollout capabilities can be achieved and a strong collaboration between providers from different Member States will be ensured. By means of workload balancing among satellite providers, an EU-wide infrastructure network will be achieved.

As a result, the satellites-scenario for AI-Factories mainly provides training of small and midsized models, post training, finetuning, hosting of models, huggingface mirroring, etc. The scenario is supposed to be of high relevance for European bluechips, data center and cloud service providers, as well as SMEs, Start-ups, Campus initiatives, and industry-near research projects.

It will also have a strong positive effect on the development of AI ecosystems as well as regional hubs and collaborations networks across the EU Member States, leveraging the implementation of EU-wide AI and cloud-edge strategies. The satellites for AI-Factories will allow organizations to explore and adopt next-generation technologies, thereby enabling technological leadership in subsequent innovation waves.

3.3. Exemplary application scenario #3: Autonomous driving and advanced driver assistance systems

The application scenario for autonomous driving and advanced driver assistance systems is one of the most complex in terms of the variety of technologies and represents a significant advancement for the automotive industry. The necessary technologies address functionalities for critical safety issues with the objective to significantly reduce accidents resulting from human errors such as distraction, fatigue, or delayed reactions. Moreover, they enhance traffic flow optimization, thereby decreasing fuel or energy consumption.

The integration and efficient deployment of these advanced AI solutions into embedded (in-vehicle) and edge computing platforms must be thoroughly addressed. Therefore, the development of an integrated, end-to-end toolchain will be essential for continuous AI model training, simulation, testing, and validation throughout the development lifecycle.

Secure and reliable communication technologies, combined with robust cybersecurity practices and stringent data privacy measures, are critical to ensure the safety and reliability of autonomous systems. Infrastructure requirements include communication, data storage, and compute. Communication with edge computing platforms involves two categories of data transfer: ad-hoc communication consisting of smaller data packets e.g., below 1 MB (for triggers or targeted queries), and scheduled communication involving large data packets of 1 GB or more, such as over-the-air updates, measurement data, and logs.

Embedded computational capabilities for autonomous driving will typically require processing power exceeding 2 TFLOPS or 200 TOPS. Additional computing resources are essential, both near-premise edges and in the cloud, for simulation and validation processes e.g., for energy- and resource-saving reasons or offloading of non-safety relevant functions from the vehicle into the cloud. Therefore, transport infrastructure-based edge computing is an important aspect for AI training computing resources during development and should support baseline workloads for smaller-scale training activities e.g., requiring more than 1000 GPUs. These are typically utilized for pre-development, smaller model updates, and related tasks. Cloud computing resources, such as AI Factories, are necessary for peak workloads involving occasional extensive training sessions e.g., demanding over 10,000 GPUs.

3.4 Exemplary application scenario #4: Zero-trust scenario for privacy-preserving and governable multi-tier execution in the edge

This scenario aims to localize private and sensitive data processing — including Verifiable Credential (VC) issuance, identity resolution, and verification — at the edge of the network, under strict data governance and sovereignty requirements. Only non-sensitive metadata, credential schemas, and trust policy definitions will reside in the cloud, ensuring zero footprint of personal data in centralized infrastructures.

A federated governance framework will help to control all data flows and interactions between the cloud and edge tiers, such as metro-edge or near-premise. This includes fine-grained access control, purpose-bound permissions, and fully consented data movements, enabled through a zero-trust security model and the enforcement of zero-knowledge proof mechanisms where applicable. All data exchanges will be cryptographically signed and timestamped to ensure auditability, but without compromising sovereignty or locality of sensitive data assets.

To ensure semantic transparency and traceability, the architecture will integrate an ontology of identities and entities involved across tiers (issuers, holders, verifiers, registries, and governance nodes), based on W3C and blockchain nodes aligned vocabularies. This ontology will support automated reasoning and policy enforcement at runtime, enabling self-describing and self-auditable transactions as well as compliance proofs.

4. Definition Types of Infrastructures

Category		Type	Power capacity	Latency	Distance	Availability
Cloud	Cloud	In-country data centers	up to 50 MW	≥ 20ms	≥ 1000km	≥ 99995%
Edge	Metro - edge	In-country data centers	up to 15 MW	≤ 20ms	≤ 1000km	≤ 99995%
Edge	Medium - edge	Near edge	up to 5 MW	≤ 10ms	≤ 500km	≤ 99995%
Edge	Medium - edge	Far edge	up to 1 MW	≤ 5ms	≤ 100km	≤ 99982%
Edge	Medium - edge	Near-premise	up to 200 KW	≤ 1ms	≤ 5km	≤ 99741%

Table 1: Categories of types of infrastructures

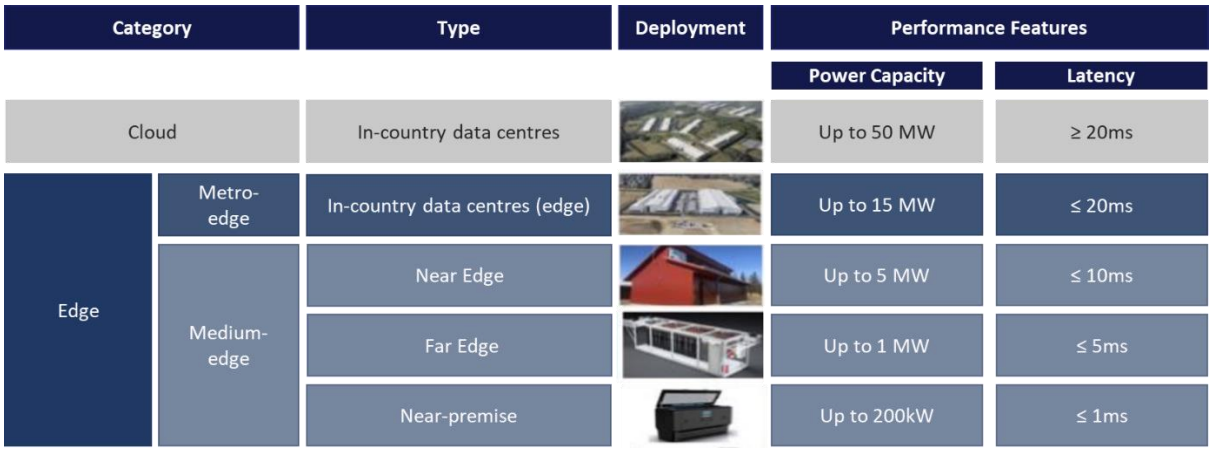

Figure 1: Overview of types of infrastructures[4] (adapted version)

[4] https://ec.europa.eu/newsroom/dae/redirection/document/104556

Cloud (Up to 50 MW, ≥ 20ms latency)

Type of edge node: In-country data centers

Hardware features: Large facilities containing lines of racks of standard servers, accelerators, and other IT components.

Software architecture: Bare metal, VMs, clusters, containers, all architectures, all services. Linux and Windows.

Metro edge (Up to 15 MW, ≤ 20ms latency)

Type of edge node: In-country edge

Hardware features: Large facilities containing lines of racks of standard servers, accelerators, and other IT components

Software architecture: Bare metal, VMs, clusters, containers, all architectures, all services. Linux and Windows.

Near edge (Up to 5 MW, ≤ 10ms latency)

Hardware features: The scale of the deployment increases in number of standard servers, networking devices, and other IT components in comparison to the far edge deployment. That could also imply different cold chambers in a specific facility or in a close group of facilities.

Software architecture: Virtualized, containerized and clustered compute. VNF, CNF, managed services, and networking. Linux and Windows.

Far edge (Up to 1 MW, ≤ 5ms latency)

Hardware features: Number of servers and networking devices with accelerators are increasing. Network elements and other IoT components are also scaled up as the data center grows.

Software architecture: Virtualized, containerized and clustered compute. VNF, CNF, managed services, and networking. Linux and Windows.

Near-premise (Up to 200 kW, ≤ 1ms latency)

Hardware features: Limited number of standard servers and networking with accelerators

Software architecture: Virtualized, containerized, and clustered compute. Working on Linux and Windows.

5. Open and non-discriminatory access to infrastructure

The obligations to grant open and non-discriminatory access to the infrastructure, and non-discriminatory pricing and network operation, as laid down in point 45 of the IPCEI Communication from the Commission C (2021) 8481 applies to each single participant in the CIC IPCEI.

Operationalization will be discussed during the design phase.

6. European Dimension of the Deployment

The federated and distributed infrastructure to be deployed in the IPCEI-CIC represents a European network consisting of cross-border connected regional segments. Therefore, the cross-border interconnection of the deployed infrastructure and collaboration among all involved parties is an indispensable prerequisite. This means that the cross-border interconnection between all components

must adhere to common processes. All components have to be compatible with each other to allow for a seamless transfer of workloads and a seamless deployment of applications to any node (of the same category) the network has to be enabled.

As an operationalization of this concept, all hardware resources must be able to serve as deployment basis for applications, which are developed according to the Cloud-Edge Continuum Reference Architecture of IPCEI-CIS. This reference architecture has a modular design encompassing the entire cloud-edge stack: It spans from physical and virtual infrastructure to orchestration, platform services, data handling, and artificial intelligence, each layer designed for interoperability in distributed, multi-provider environments.

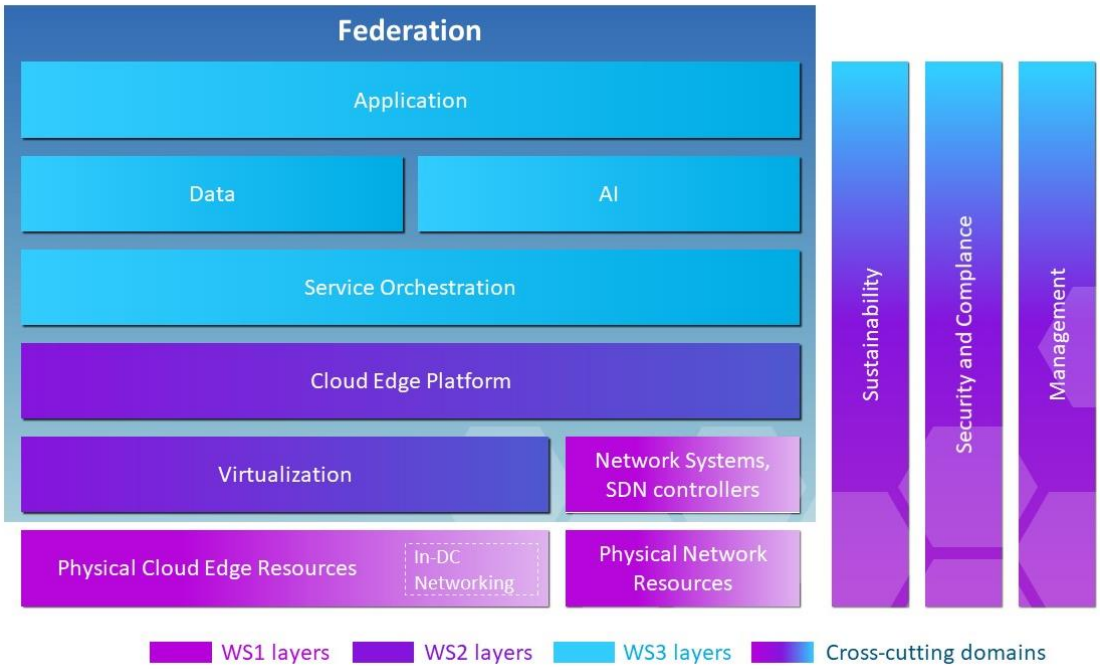

Figure 2: Reference architecture model of cloud-edge continuum (IPCEI-CIS)

7. Related Initiatives

Initiatives related to IPCEI-CIC objectives should be taken under consideration and linked to improve the efficiency of the deployment of infrastructure nodes, such as:

- IPCEI-AI
- AI-Gigafactory
- IPCEI-CIS (8ra-initiative)
- AI software development
- IPCEI ME/CT
- EU Silicon development
- EURO HPC
- AI On Demand Platform
- Simpl
- 5G corridor EU initiative

8. Roadmap

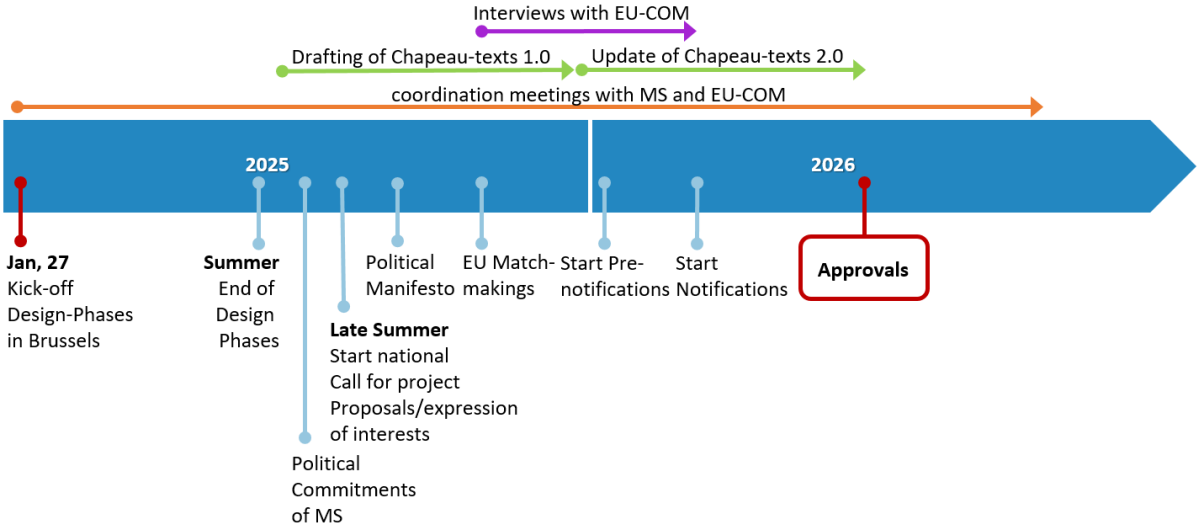

Figure 3: Illustrative roadmap with important milestones of IPCEI-CIC; final date for approval depends on further processes