IPCEI on Next Generation Cloud Infrastructure and Services (IPCEI-CIS)

Working Paper

- Value Chain Desciption -

Outline

1. Introduction

To seize the data opportunity and optimally respond to end-users' expectations in terms of computing capabilities, real-time, ultra-low latency, data security, interoperability, sustainability, the European Union (EU) needs to become a global leader in federated data processing (cloud and edge) capabilities. The EU needs to invest into the development (including industrial research) and first industrial deployment of the next generation of cloud-edge capabilities to foster among others new types of data and platform solutions.

The EU needs to rely upon a self-sustained and efficient utilization of cloud-edge provider ecosystems to foster resilience and technological leadership. By supporting the development of federated data management system, existing data resources in the EU can be used swiftly, data processing capacities can be used efficiently, and new business models will be possible based on ultra-secure data communication, real-time capability in data provision, new data processing services and on a sustainable energy-efficient data usage. This will enable EU data spaces to connect to the next generation of green data processing solutions, to increase reliability, performance, scale and to decrease costs for users and providers. The IPCEI will leverage existing initiatives on EU and national level especially the GAIA-X open source architectural framework.

At the core of the next generation cloud to edge capabilities is the "Distributed Multi Provider Cloud-Edge Continuum", which is composed of a common distributed data processing infrastructure with platform and service functionalities that aim at:

- High scalability in a multi-provider environment across the EU
- Guaranteed latency and bandwidth
- Ultra-secure infrastructure and services aligned to EU rules and values
- Data exchange in ultra-low latency for added value creation
- High interoperability and portability of services and data among all cloud-edge users and providers enabling seamless shifting between providers and overcome vendor lock-in for users
- Sustainable and energy efficient data processing capacities enabling new innovative, green business solutions and process efficiencies
- Development of cutting-edge smart processing and networking services
- Promoting standards where appropriate
- Creation of common set of tools and services (AI, IIoT/IoT, analytics etc.)
- Development and enhancement of innovative open source cloud-edge technologies

The goal of the integrated IPCEI-project is thus to develop and initially roll-out the key interdependent building blocks and the associated horizontal requirements (such as sustainability, cybersecurity) along the strategic steps of the value chain of the Distributed Multi Provider Cloud-Edge Continuum. Such a continuum will be based upon a common end-to-end data processing infrastructure, enabling value creation via providing platform and application services across the EU, fulfilling key requirements of ultra-low latency, dynamical bandwidth and cybersecurity. The IPCEI will interconnect cloud-edge computing by establishing the multi-provider cloud-edge continuum as technological basis for the initial roll-out of advanced data processing capabilities for key sectors such as automotive, manufacturing, energy, logistics, transport/mobility, tourism, education or public services (smart cities, health, etc...). The multi-provider cloud-edge continuum will deploy key digital technologies and applications like smart networks and services (e.g. AI, analytics), data driven robotics, common generic data space applications and cloud-edge foundation services. The IPCEI-CIS will accelerate the cloud-edge uptake among SMEs, industries and public administrations by adressing emerging data processing demand and foster the EU global technological leadership in the cloud-edge sector.

2. Value Chain Steps and Building Blocks

The common next-generation cloud-edge infrastructure and its associated smart platforms and services to be rolled out across the EU - consisting of hardware packages[1], infrastructure-related software, meshed compute facilities and smart platforms and services - must be open, highly efficient and secure. It includes among others cloud hardware components such as computers and networks, associated software components and services as well as platforms and sector agnostic services.

The integrated IPCEI-project will enable to scale up and guarantee the interoperability of application software and data delivered by the providers on top of the infrastructure. At the same time, this infrastructure must be federated and equipped with innovative cloud-edge computing platforms, integrated smart network to cloud services and added value data processing services so as to enable the connections between cloud-edge computing to become a continuum (Multi Provider Cloud-Edge Continuum). Technological features and Research, Development and Innovation (R&D&I) aspects will be logically combined according to vertical and horizontal building blocks to structure the integrated IPCEI-CIS value chain.

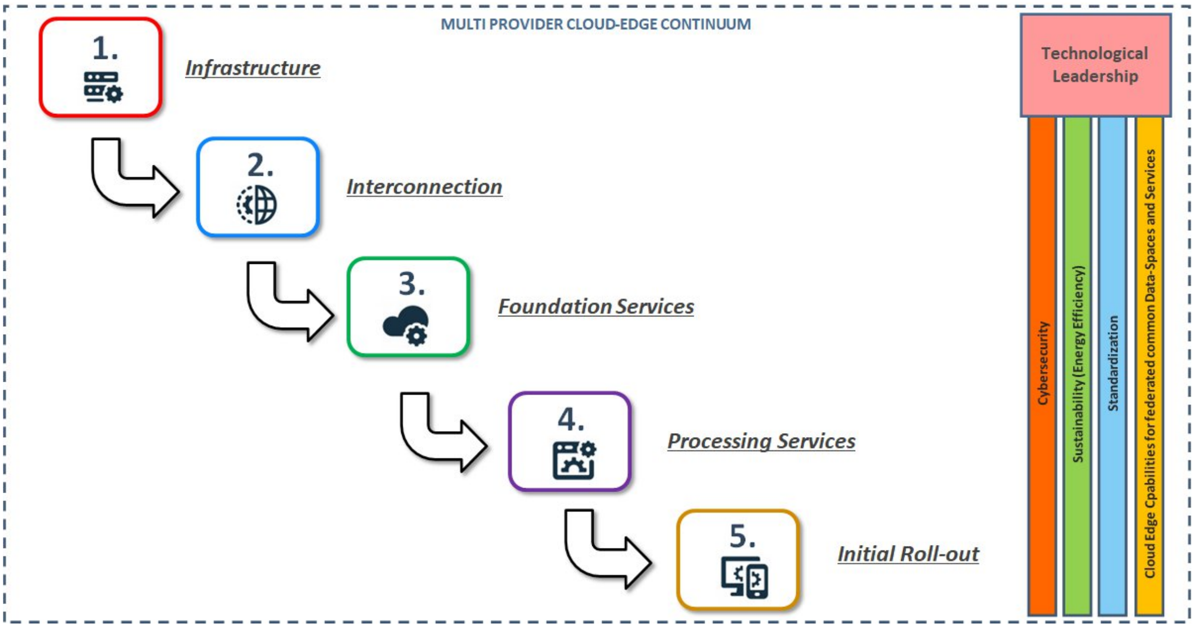

Figure1: Value Chain Steps

In each building block of the value chain and along the entire technology stack interoperable, reliable and measurable framework conditions in relation to cybersecurity, sustainability, standardization and capabilities as traversing requirements for a trusted cloud-edge continuum need to be guaranteed. The identified key building blocks and horizontal requirements along the value chain are:

- (1) Infrastructure - Setting up an appropriate and supported next generation infrastructure (forward-looking data center facilities, servers, storage, mobile and fixed/stationary interconnections) to manage the technological complexity of the meshed continuum.

[1] Composition of compatible hardware components of the Multi Provider Cloud-Edge Continuum as basis for the operationalization of next generation data processing capabilities.

- (2) Interconnection[2] - Develop and set up of physical and logical linking of networks including integrated smart network services for the cloud-edge continuum. This will enable the entire network to combine cloud-edge computing processes and data transfer throughout the EU.
- (3) Foundation Services – The development of infrastructure related services to run on the multi-provider cloud-edge continuum is the basis for real time data services with ultra-low latency and the load balancing for optimised utilization. This will enable sorting, interpreting and prioritizing the storage and processing capabilities of large amounts of data in advance as close as possible to the place of origin and/or consumption of that data.
- (4) Platforms and Smart Processing Services - Provide integrated services such as application lifecycle management to build, deploy and maintain apps all over the cloud-edge continuum - platform services -; data management to ease data ingestion, transformation and analysis in a multi-provider, federated environment in accordance with European regulation - data platform; and innovative data processing leveraging AI and ML - smart processing services -
- (5) Initial roll-out of next generation use cases as part of a first industrial deployment with European wide scale, showcasing data processing in different sectors to verify functionality, high scalability, interoperability, portability, interconnectivity and compatibility.

The continuum will provide users and service providers equally with the appropriate infrastructure, platform services and a beyond state-of-the-art governance for a digital data management, enabling the next generation green data processing solution of tomorrow which guarantees

- Cybersecurity
- Sustainability (Energy Efficiency)
- Standardization
- Cloud Edge Capabilities for federated common Data-Spaces and Services

Outlook potential IPCEI-CIS Building Blocks

Efficient, high-performance, highly secure, federated next generation cloud infrastructure and services must flexibly integrate all data sources, data connections, computing units and data storage options. Therefore, a common perspective on the technological architecture and potential building blocks of a Distributed Multi Provider Cloud-Edge Continuum will be developed as an integrated IPCEI project. This continuum covers devices, near and far edge nodes, central cloud data centers as well as the integration of specialized data centers (e.g. HPC) and smart networks. This will enable the development and distribution of smart data and innovative services, like swarm and fog computing across the continuum.

The integrated project needs an appropriate technological framework to guarantee a successful set-up and roll-out based on the following targets in a multi-provider environment:

- Create a common architecture with technological components for an open cloud-edge stack which is highly scalable and interoperable
- Create a set of services to automate in the highest possible scale the federation/orchestration at cloud-edge level
- Enable Security Operation Center (SOC) and Computer Emergency Response Team (CERT) to be able to serve customers' needs and security accidents from edge to cloud across national borders
- Create an automated management for distributed hardware

[2] Interconnection refers to the physical and logical linking of networks with equipment or facilities not belonging to the administrative domain of that network. This includes the interconnection of carriers, cloud service providers, content delivery networks, mobile and fixed-line network service providers, and other participants of the Internet and (edge) cloud continuum running networks (e.g., data centers, enterprise networks). The resulting composed infrastructure layer is a critical building block required for a multitude of network services, existing and new applications implementing various end-to-end scenarios in the Internet and (edge) cloud continuum.

- High level of energy efficiency and security across all technology building blocks
- Create platform and smart processing services to support different applications (easy, fast, secure, reliable data exchange and sharing)
- Ensure interoperability and platform scalability and
- Overcome users' vendor lock-in and foster data portability

The graph displays potential building blocks of the Multi Provider Cloud-Edge Continuum which will be further elaborated with the successful project applicants during the notification of the integrated project:

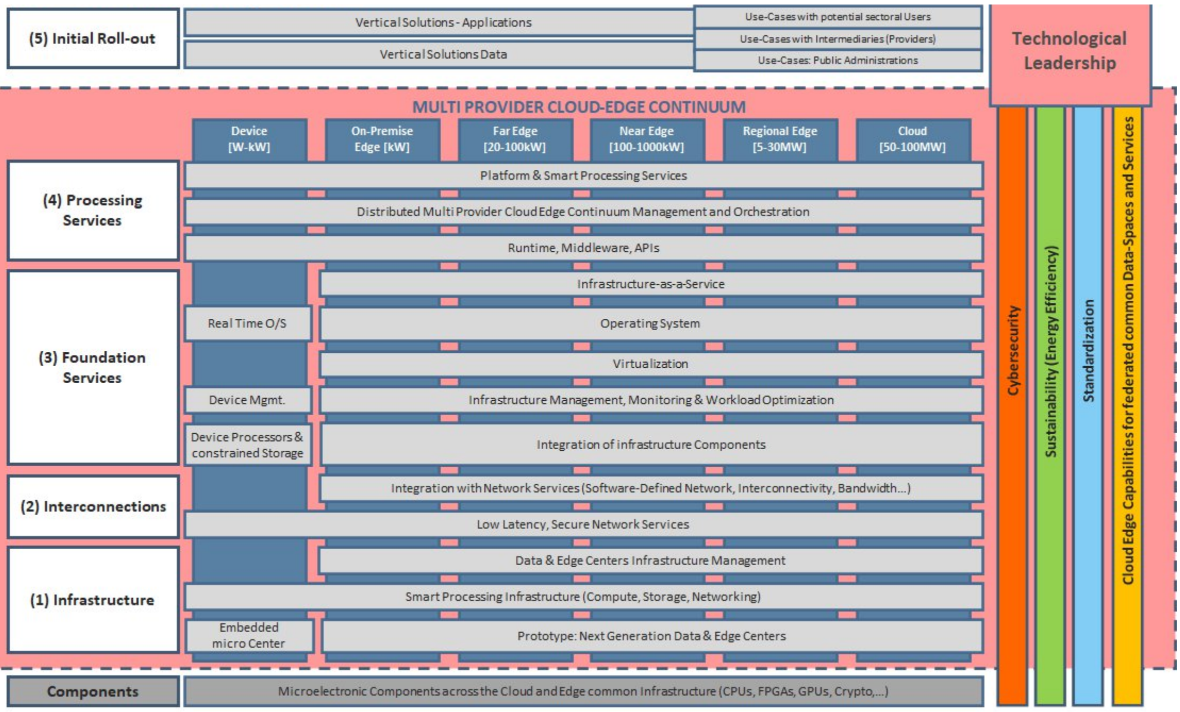

Figure 2: Building Blocks of the Value Chain

Legend:

2.1 Infrastructure

Next generation data processing needs suitable and highly scalable software and compatible hardware packages, this implies central cloud computing capacities, regional edges, far edge and near edge data centers, fast energy-efficient next generation processors for data processing and communication as well as dedicated components for real-time and security-critical data transfer operations. The infrastructure for a multi-provider cloud-edge continuum and the applications and services running on it are scalable, compatible and interoperable hardware packages and infrastructure related software.

This may include the complementary linkage to other EU initiatives focussing on energy-efficient microprocessors, components for real-time and safety-critical operations, microelectronic components for 5G and the future 6G, integrated circuits with specific functionalities (e.g. secure crypto-processors), sustainable edge-cloud data center facilities and the integration to telecommunication infrastructures to connect users and nodes in the cloud-edge continuum.

Additionally, the roll-out of the future EU common data processing infrastructure will require the integration to smart networking services based on significant enhancements in terms of transmission rates, latency, energy consumption, data integrity, reliability, and security for the deployment of critical applications and services. This will also require the evaluation of cutting-edge processors with advanced features; highly secure chips and quantum communication modules; faster and higher-capacity storage units, allowing the use of big data and AI/ML in an increasing number of applications and advanced switching and routing devices with extremely high transmission rates.

IPCEI-CIS will include the development and first industrial deployment of cloud-edge nodes co-financed by public and private stakeholders, addressing the specific needs of end-users located across the EU Member States. These investments may cover the entire cloud-edge categories, with a specific focus on supporting the initial development and deployment of the cloud-edge facilities. This will contribute to the EU target of deploying 10,000 climate-neutral highly secure edge nodes by 2030, guaranteeing equal access to data services with low latency (few milliseconds) wherever users are located[3].

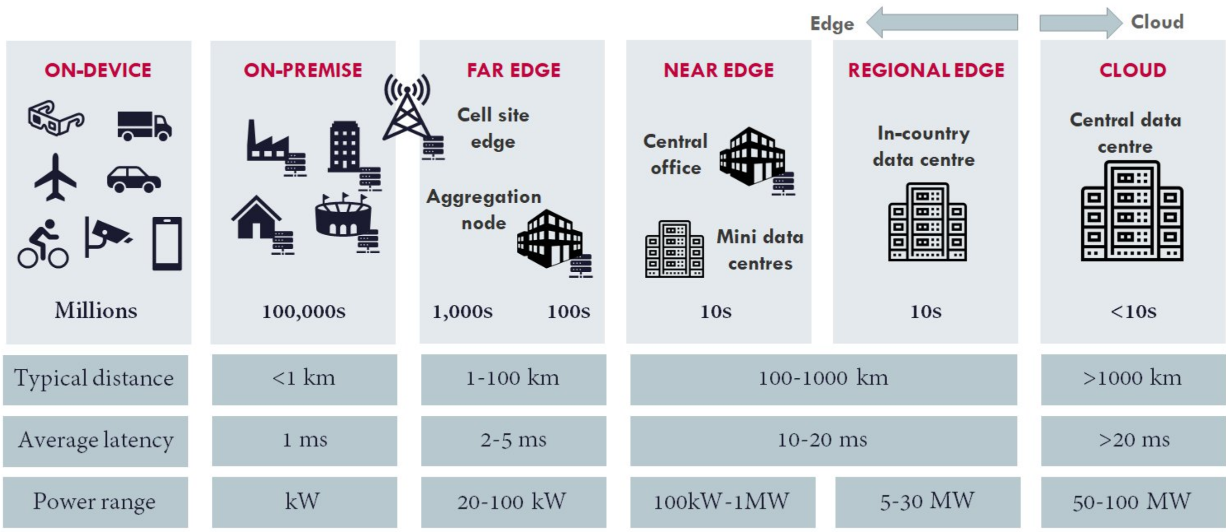

Figure 3: Cloud-edge categories and characteristics[4]

IPCEI-CIS will offer the possibility to migrate existing cloud capabilities to connect to the Multi Provider Cloud-Edge Continuum to develop and firstly deploy next generation cloud infrastructure and services with edge nodes, specifically:

- For providers of future central data centers in the EU, the infrastructure will enable significant data processing capability sharing.
- Near-edge cloud capabilities will contribute to the first deploying of several hundreds of nodes with latencies below 20 milliseconds.
- Far-edge capabilities with thousands of nodes, will get closer to the customer and will deliver latencies of a few milliseconds.

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "2030 Digital Compass: the European way for the Digital Decade", COM(2021) 118 final

[4] European industrial technology roadmap for the next generation cloud-edge offering https://digital-strategy.ec.europa.eu/en/library/today-commission-receives-industry-technology-roadmap-cloud-and-edge

The IPCEI-CIS will evaluate emerging and existing hardware packages as well as necessary research to guarantee secure and reliably available data processing, storage and transmission for the next generation European cloud infrastructure and services[5]. R&D&I activities will include the design, development and integration of innovative hardware packages.

The IPCEI-CIS will also encompass activities related to infrastructure management across the continuum.

- At near-edge locations, advanced technologies for management, real-time monitoring and workload optimization will be implemented, including cutting-edge AI and ML-based tools.
- At far-edge locations novel approaches related to devices and edges and their integration will be considered.

In this sense, the next-generation cloud-edge nodes will take advantage of disruptive technologies such as improved high-density storage solutions. Specific data compression software will also be developed for computationally intensive tasks on the edge (e.g. real-time video analytics). This should be complemented by a strategy that aims for a more efficient distribution of data across the continuum, bringing critical data closer to the user.

Besides the federated data processing infrastructure development, the development of an advanced data center and edge center infrastructure management tool, that would strengthen the operational efficiency of European cloud-edge offerings, is a main requirement as well. AI and ML are key technologies that must be developed and implemented to optimize the data center infrastructure.

Possible common infrastructure management tools could be used for the next generation cloud-edge offering[6]:

- Computer Fluid Dynamics (CFD) simulations to optimize rack layout in the data halls.
- Building Management Infrastructure (BMS) for real time monitoring of data center installations, power consumption, and climate impact.
- Data Center Infrastructure Management (DCIM) for monitoring, Power Usage Effectiveness (PUE) management, operation, capacity, change space and network and Robotics Process Automation (RPA).
- To use tools instead of manual tasks avoid human errors in operation and monitor data center working conditions continuously. Artificial intelligence and machine learning provide the ability to analyse data center infrastructure data and provide insights and guidance on measures to improve the operational performance of data centers and reduce energy consumption.
- Technologies which contribute to enhance transparency, traceability, time stamping and self-execution of smart contracts, which will additionally contribute to operationalize performance of sustainable data processing.

The use of these management tools to optimize the entire infrastructure and operations of data centers is a growing area of development where the EU can apply its existing capabilities.

2.2 Interconnection

Robust and high-speed connectivity across Europe, not only in well-connected urban areas and industrial hubs, but also in remote and rural zones, is a key enabler for the development of next-generation cloud-edge services available to all EU businesses and citizens and paths the way to EU digital single market. Thus, adequate connectivity with ubiquitous access to low latency will have to be

[5] IPCEI-CIS activities will not cover development or manufacturing of individual components.

[6] European industrial technology roadmap

considered for the federation of different providers of cloud-edge computing at network level and to connect all edge nodes to the cloud-edge continuum.

Next generation smart processing infrastructures will progressively rely on cloud-edge capabilities, edge devices and Internet-enabled mobile devices. These infrastructures will enable the management of user-oriented interconnectivity[7], interoperability and data or service portability, specific requirements with regard to end-to-end security, low power and ultra-low latency in data transfer and storage, bandwidth availability and load balancing in a complex multi-provider environment. The next generation of physical and logical interconnection, including cloud-edge and telco infrastructure, will bring data processing solutions closer to where end users are physically located across the EU with the guaranteed performance (eg. latency, bandwidth). For this sake, the fixed, mobile and backbone networks will have to adapt different domains, from access to core. The composed infrastructure layer is a critical building block required for a multitude of network services, existing and new applications implementing various end-to-end scenarios in the Internet and (edge) cloud continuum. All this ensures that users get appropriate access to the cloud-edge continuum.

The IPCEI-CIS will pursue technologies that allow multi-vendor radio access solutions to boost next generation mobile networks. In this regard, mobile network operators and sectoral stakeholders are exploring an evolution towards open virtualised models for the radio access network, built on off-the-shelf hardware and cloud-based software in a multi-vendor environment with open and standard interfaces between network elements. This paradigm can have a significant impact, allowing new equipment vendors to enter and compete in the market, enabling faster software innovation, allowing more network flexibility, and facilitating network exposure to third-party edge applications through open Application Programming Interfaces (APIs).

This new architectural concept requires a cloud environment at the edge to host some of the network functions traditionally located at the base station, becoming an important tenant of the edge cloud. Improved network architectures will be required to support the intended widespread of cloud-edge services across the value chain. This relates to the growing use of big data in many sectors, which translates into an increasing demand of network capacity (bandwidth); backbone elasticity; the exponential rise of connected devices, mainly in the furthest locations of the continuum; the rapid change in network traffic patterns, which demand more flexibility in interconnection; the emergence of time-critical or automated applications with strict quality of service (QoS) requirements; threats to privacy requiring end-to-end security; etc.

The IPCEI-CIS will research and implement novel strategies for network management, aiming at improved network performance, more flexibility and easier monitoring to enable real-time data processing along the cloud-edge continuum. Technologies such as Software Defined Networking (SDN) will be particularly suited for self-service provisioning across the cloud-edge continuum, allowing elastic scaling of computing, storage, and network resources. The integration of SDN has the potential to provide edge and mobile edge orchestration and a dynamic configuration of the underlying interconnection infrastructure for improved service continuity and QoS across the cloud-edge continuum.

These cloud capabilities of transport connectivity and related network resources can be exposed as a Network-as-a-Service (NaaS)[8], allowing the cloud service customer to provision network services and resources, as needed, automatically or with minimal interaction with the NaaS cloud service provider.

---

[7] Interconnection refers to the physical and logical linking of networks with equipment or facilities not belonging to the administrative domain of that network. This includes the interconnection of carriers, cloud service providers, content delivery networks, mobile and fixed-line network service providers, and other participants of the Internet and (edge) cloud continuum running networks (e.g., data centers, enterprise networks).

[8] As defined by Rec. ITU-T Y.3515 “Cloud computing – Functional architecture of Network as a Service”

2.3 Foundation Services

An increasing number of real-world applications, including industrial processes, require the execution of highly specialized functions quickly and without errors. These applications need a high automation degree, transmission and storage of high data volumes, real-time with guaranteed latency and bandwidth in data transfer and processing, reliability, resilience, access control, and energy-saving options. Cloud-edge computing creates an everywhere available and continuous computing environment. It is expected to optimize significantly the following aspects:

- Overall performance and latency improvement of the system, minimisation of network traffic, energy consumption and data transfer costs, add reliability to the cloud-edge continuum
- Provide guarantees for data privacy to comply to GDPR and other data protection and privacy policies

Foundation Services

Foundation services are the basic infrastructure services upon which smart services are built and thus have a crucial role in the technological stack. From the user's perspective they impact the resilience, trustworthiness, reliability, adaptability, cost-effectiveness and performance needed to create innovative applications. Elasticity, the capability of scaling up infrastructure to meet demand, is further characterized by ramp-up time in which new resources can be brought on, typically ranging from minutes for virtual servers, seconds for micro-service containers, and tens of milliseconds for functions. The foundation services can be open source to enable collaborative development, high usage rates and transparency for operations. In addition, foundation services like workload optimisation are needed to connect the different layers of the cloud-edge continuum.

Continuum Control Functions

The efficient use and distribution of required resources is an important factor when operating a multi-provider cloud-edge infrastructure. With cutting-edge methods like provision and evaluation of telemetry, the utilization of the infrastructure can be increased. To operate this new type of continuum, it is necessary to collect a large set of telemetry data that is kept under lock and key in conventional infrastructures. Relevant metadata can also be made available to the user and service provider.

The following control functions are essential to operate the future continuum:

- Scalable edge-cloud hardware fleet/resource management
- AI driven workload management
- Lifecycle management and workload optimisation
- Effective resource monitoring and scheduling
- Deep telemetry component monitoring
- Edge identification and monitoring
- AI driven predictive maintenance
- Meta data transparency
- Reusable framework based on open interfaces and components

Next Generation Cloud-Edge Operating System

In a complex multi-provider cloud-edge continuum (Mesh), a new type of highly automated Operation System to ensure coherent application behaviour by managing dynamic loads, disaster recovery, utilization and resource allocation as well as energy efficient operations. This future Operating System has the capabilities of executing requests on edge nodes without buffering delays and will work in synergy with virtualization layer to fulfil the ultra-low latency requirements. It will also enable resource splitting amongst different operating systems, through which CPU cores and chunks of memory assignment becomes seamless to different operating systems to make sure that RT parts are always on time, while maximum throughput is still available for the rest of the system. Reliability and resilience of the system is also assured: one OS can crash while the others are unaffected. With high degree of customisability and it should be used in different configurations.

API-Framework

A common API framework is necessary for the development and maintenance of applications and services within the cloud-edge. The API framework needs to cover cloud, edge and a broad set-up of providers functionality. It is important to support existing frameworks and be expandable based on new cloud-edge requirements. Basic elements are:

- Reference API gateway to secure and route API requests
- End-to-end orchestration
- Analytic functions for reporting
- Location and performance
- Multi-provider cloud-edge load balancing
- Multi-provider data and service portability
- API Portal to register and maintain API services and for collaboration and documentation

Virtualization and containerized Workloads

To independently run critical infrastructure services safely it is necessary to care for virtualization of the edge and cloud computing resources within the multi-provider cloud-edge continuum, that includes servers, storage, and networking resources. It allows centralization of administrative tasks while improving scalability and overall hardware utilization by sharing the same physical resource among many tenants. With virtualization, several operating systems can be run in parallel on a single server. The development of the next generation virtualization layer is a combination of software-defined compute, storage and networking in modest scale for edge and vast scale for clouds. Virtualization enables the management and operations of the virtual and containerized workloads. The virtualization layer will enable multitenancy and interoperability to provide an all-purpose standard technical specification and interface for the integration of existing and future components of the cloud-edge continuum into an efficient and replicable cloud virtual infrastructure layer.

A key aspect of virtualization is that it enables effective Container-as-a-Service (CaaS) implementations and the orchestration of these CaaS may be deployed on heterogeneous systems using open standards. In this way applications may be set-up on the continuum from multiple vendors, dynamically tailoring deployment according to needs and opportunities.

2.4 Platform and Smart Processing Services

On top of core foundation services, added value services are required to extract the full value of the multi-provider cloud-edge continuum. Those platform services bridge foundation services with end users' applications, can ease application lifecycle management, resources and services orchestration or provide innovative processing capabilities - called smart processing services in the case of the integrated IPCEI-CIS project.

Platform Services

The next generation platforms services ensure real time requirement for applications and perform various task in multi provider environment in a seamless and interoperable manner. One of the most common type of platform services are cloud-based services through which the provider offers to a user environments and tools for developing, deploying and managing applications. As the cloud-edge continuum integrates diverse physical components from central cloud servers to edge devices, high end platform services are needed to orchestrate resources and services and to manage applications deployed in the continuum. This new generation of platform services could leverage analytic tools, like AI or digital twin, to optimize cloud and application management. Because those platform services tend to ease developers works by automating tasks they would need to do manually (e.g. application life cycle management) they are considered as essential to adoption. Those platform services could also be used as common, 'generic' services to enable the building of data spaces. Moreover, integrated smart processing services will be leveraged by the initial roll-out and use cases.

Data platforms

Data platforms ease data management by providing an environment of tools to ingest data, store it, for instance in data spaces, transform it to be able to feed it in business intelligence or tools for data science. Future data platforms need to cope with the model of the Multi-Provider Cloud-Edge Continuum where data is not anymore centralized. In particular, this requires standards that facilitate a controlled, secure and trustworthy data exchange between the decentralized nodes in this continuum. This new generation must also allow customers to manage access and control over the data (in particular depending on where the data is processed and which controls are applied) and provide tools to ensure compliance with GDPR in a multi-provider environment.

Smart Processing Services

To utilize the full value of the data managed in a cloud-edge continuum, a next generation of new and open smart processing services are needed. Those services, using innovative approaches like AI routine, digital twins, simulation and modelling or other digital technologies allow users to manage their data. Those smart processing services need to solve the trade-offs between the effectiveness of algorithms, the required memory and compute resource as well as the guaranteed latency and bandwidth, while keeping the required privacy level.

The next generation cloud-edge continuum based on middleware applications and runtime environments will enable a secure and sustainable transport of complex data. Smart processing services help to perform interconnection between the network components, ensure transaction security via monitoring, perform the pseudonymisation for identification purposes and are used to get information from data analytics. Those services are essential for the decentralisation of computing where data location and transfer through the multi-provider cloud-edge continuum in a secure, fast and reliable manner is crucial.

Federated Learning Example

To make predications in trained model for machine learning needs to involve data pipelines that are using central servers (on-premise or cloud). The downside of this architecture is that all the data collected by local devices and sensors are sent back to the central server for processing, and subsequently returned to the devices. Today, this type of data exchange limits the ability of machine learning algorithm to learn in real-time. Federated learning, in contrast, is an approach that downloads the current model and computes an updated model at the device itself (such as edge computing) using local data. These locally trained models are then sent from the devices back to the central server where they are aggregated, i.e., averaging weights, and then a single consolidated and improved global model is sent back to the devices. Federated learning will enable robust models integrating edge computing devices and services, and exploiting large distributed datasets with privacy constraints, in particular those associated to health data.

The next generation of platform services, integrated smart processing services to the cloud-edge continuum will generate added value in different sectors due to the following factors:

- They will ensure ease developers' work and provides adaptable high value services
- They will go through the whole multi-provider cloud-edge continuum enabling an integrated approach
- They will be by design fully compliant with the EU jurisdiction and European values
- They will be highly scalable, interoperable and portable
- They will contribute to data protection and data portability by easing data management
- They will reinforce their resilience due to automated application life cycle management
- They will manage and optimize energy consumption and increase energy efficiency

2.5 Initial Roll-out

The progress made in terms of connectivity, latency, data exchange, data processing and computing capabilities through the Multi Provider Cloud-Edge Continuum enable the deployment of innovative use cases at first industrial deployment stage. The initial roll-out will showcase a high scalability, security and interoperability of services and data in different domains, like manufacturing, energy, mobility, health and public services that are highly sustainable.

A wide variety of sectors can benefit from digital twins, virtual factories, remote operation and assistance, autonomous robots and other innovative services. The digitalisation of those sectors and industries will generate enormous amounts of data that can be used to maximize economic value. The sharing of data and its combined exploitation through advanced techniques of data analytics and AI, will allow companies and public administrations to build tailored products and services for business users, public administrations and citizens.

2.5.1 First Industrial Deployment (FID)

The IPCEI-CIS will include the implementation of a first industrial deployment with different use cases. This will boost adoption by users and providers, raise awareness and showcase the functionalities of the next generation multi-provider cloud-edge continuum.

Use cases to be implemented as a first industrial deployment must facilitate the development of new products and services with high research and innovation content and/or the deployment of fundamentally innovative production processes. The development of newer versions of existing products do not qualify.[9]

This first industrial deployments will allow participating project partners to deploy and test their use cases in a production environment but will not encompass mass production. This will give participants the possibility to go one step further than in large scale pilots and demonstrators.

2.5.2 Potential Use Cases

In the course of the integrated IPCEI-project use cases in areas of common European interest to foster technological leadership will be focussed. These next generation use cases can address the entire or

[9] First industrial deployment refers to the upscaling of pilot facilities, or to the first-in-kind equipment and facilities which cover the steps subsequent to the pilot line including the testing phase, but neither mass production nor commercial activities. Communication from the Commission — Criteria for the analysis of the compatibility with the internal market of State aid to promote the execution of important projects of common European interest (europa.eu)

single steps of the IPCEI value chain to consequently strengthen and build-up the cloud-edge continuum by implementing e.g multi provider load balancing, automated operations (by optimizing latency and bandwidth), disaster recovery, utilization and energy efficiency. Those use cases will include collaboration between large industry, academia, start-ups and spin-offs within specific sectors as well as across sectors. The use cases shall spill-over across Europe and foster scalability.

Potential cutting-edge use cases may address the following users and market participants:

- Potential sectoral users
- Public administration
- New types of intermediaries for creating innovative business models for data and cloud ecosystems

3. Accompanying Measures

In order to foster technological leadership IPCEI-CIS will also include accompanying measures in each step of the value chain and along the building blocks of the entire technology stack to ensure interoperability, cybersecurity, sustainability, and standardization as horizontal requirements for a trusted multi-provider cloud-edge continuum.

Technological leadership

To become a global front runner the EU should develop next generation cloud-edge infrastructure solutions that respond to the needs for cloud based applications of industries and other users like governmental administrations that were accentuated since the Covid-19 pandemic.

In the context of the IPCEI-CIS *technological leadership* should be understood as the combination of 3 concepts: resilience, data sovereignty and technological readiness.

Resilience by design:

From the user's point of view, resilience of cloud infrastructure and services is a key concern. Cloud applications should not put at risk by political changes, environmental disaster, local energy grid blackout or cyber-attacks. To ensure resilience in cloud-edge continuum applications should be deployed in heterogeneous and less centrally controlled environment.

Data sovereignty by design:

The IPCEI-CIS will ensure data sovereignty across the EU, to enforce the development and availability of open cloud applications under EU jurisdiction, especially the General Data Protection Regulation (GDPR) and the adherence towards European values.

Technological readiness by design:

The EU will gain technological readiness by fostering R&D&I in key enabling technologies by developing innovative and interoperable products and services for a multi- provider cloud-edge continuum. The IPCEI-CIS will strengthen Europe's technological readiness for open, transparent and sustainable cloud-edge technologies even to be operated worldwide.

3.1 Cybersecurity

End-to-end security is necessary while sharing resources and co-locating network functions. Application services require means in infrastructure management tools to offer secure deployment that minimises risks of data privacy or integrity breaches. By taking the approach of using compute resources outside of the well-established data center security controls, security challenges emerge both at the level of digital and physical security. These encompass the need of security measurements for cloud-edge infrastructures at the levels of connectivity. In addition, security controls need to be designed with high degrees of compatibility in mind, due to the high heterogeneity of the devices and environments to be protected. These are combined with strong requirements for data security and privacy in the data management.

Cybersecurity is a key aspect along all layers of the Multi-Provider Cloud-Edge Continuum to guarantee trustworthiness, traceability, resilience and reliability among users and providers. Security solutions in a next generation cloud-edge continuum should provide multiple layers of trust in the hybrid multi-cloud environment that helps organizations to maintain full control on the security and protection of their data in the cloud-edge continuum, via for example:

- Implementing identity, attribute, signature and zero trust access management, Public Key Infrastructure (PKI) management solutions compliant with EU rules and standards (such as eIDAS, Decentralised Identifiers (DID[10]) support, ...).
- Applying HSM based solutions to secure data in transit and at rest. Robust and reliable symmetric, asymmetric and post-quantum crypto technologies.
- Implementing solutions to secure data in use (for example confidential computing, polymorphic encryption)
- Using trustworthy and secured and EUCC[11] certified hardware (secure boot/update, firmware integrity validation, disk encryptions, physical security/hardening, compliant with secured HW management standards – RedFish-...)
- Applying the European Cloud Certification Scheme[12]
- Implementing responsible vulnerability disclosure schemes
- Implementing threat information and intel sharing mechanisms
- Implementing collaborative risk management for objective estimation and evaluation of cascading and systemic risks

IPCEI-CIS should support the development of next generation cloud-edge security solutions enhanced by AI capabilities that provide a single pane of glass in security controls making sure security policies are consistently deployed across the heterogeneous cloud environments, providing necessary netflow data and auditable evidence to all relying parties. This may include prescriptive security services, for example Security Operation Centre (SOC) services such as MDR solutions (managed detection and response).

IPCEI-CIS should develop the next generation cloud-edge incident management tools and collaborative and cross-border case handling platforms making sure that incidents of any scale can be addressed in a coordinated and efficient way.

---

[10] https://w3c.github.io/did-core/

[11] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme

[12] https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme

3.2 Sustainability (Energy Efficiency)

The potential IPCEI-CIS will directly contribute to the development of green and sustainable technologies that go beyond state-of-the-art solutions available along the entire value chain steps and technological building blocks. This is fully aligned with European Green Deal considering new digital technologies to be a critical enabler for attaining the sustainability goals to transform the EU into a fair and prosperous society, with a modern, resource-efficient and competitive economy with no net emissions of greenhouse gases in 2050 and where economic growth is decoupled from resource use.

In the future, digital infrastructures in general and data centers in particular will need to be more strongly integrated into overall energy management concepts. This is also required by the EU Commission´s strategy for the integration of the energy system. The integration can create a basis for sustainable and competitive digitalisation in the EU.

In this context cloud-edge computing is a central prerequisite for ecologically sustainable digitalisation in Europe. Under the IPCEI-CIS a vast number of participating projects shall take sustainability aspects incl. optimisation of energy consumption into consideration and must ensure that no environmental harm is posed by its implementation.

IPCEI-CIS will foster advancements in computing, data storage, communications, and innovative heat removal technologies to support green service solutions across al value chain steps, for example in the areas of:

- **Optimised cooling technologies** – IPCEI-CIS may provide incentives for ideas and investments to optimize cooling systems for cloud-edge data centers, such as airflow management and design, liquid cooled server solutions, cooling management, temperature and humidity settings, the use of natural refrigerants and free cooling technologies.
- **New ways of waste heat recovery** – IPCEI-CIS may encompass the development of innovative concepts to use waste heat from data centers such as the connection to local and district heating networks to significantly improve the CO_2 balance and the sustainable operation of cloud-edge data centers (typically more than 60% of the energy in the data center is converted into heat).
- **New cutting-edge innovation to make use of renewable energy**: Data centers, regardless of their size and business model, whether edge or cloud, are not primarily CO_2 emitters, but depend always on the energy mix of the respective location. IPCEI-CIS projects may integrate and accelerate the direct use of nearby renewable energies sources in future cloud-edge computing locations (if not restricted by national regulation or state aid rules).
- **Cloud infrastructure management** – IPCEI-CIS may support the development of tools and mechanisms to optimise energy usage in the infrastructure in order to
  - assess the energy consumed in lifecycle of AI workloads (data-acquisition/preparation, training/testing/operation/optimisation) addressing different execution environments (edge/cloud/HPC).
  - optimize resource utilisation and find the best location in which to execute a workload, enabled by intelligent off-loading schemes as well as simple and transparent portability among edge and cloud resource types and models.
  - study trade-offs among energy consumption for different hardware processor architectures for exemplary models and benchmarks.
  - characterize edge devices energy consumption patterns and impact of data transmission.
  - exploit cognitive data center features to optimise energy usage in the infrastructure (such as the development of application of Machine Learning (ML) techniques in the context of HPC and enterprise environment for monitoring and supervision of energy consumption).
- **Artificial intelligence for computing resources** – IPCEI-CIS may promote energy efficient software programming (green coding) to unlock the immense potential for savings in energy consumption.

It will foster the development of tools and mechanisms for AI developers and users, as well as for infrastructure managers, to understand and optimise energy consumed by cloud-edge services and AI related processes and its associated carbon footprint in diverse cloud, HPC and edge environments (such as frugal AI, neuromorphic computing or needs-based software programming to optimize existing hardware).

- **Enacting robust data collection and open data repository systems for data center energy use** IPCEI-CIS may boost the development and open sharing of reliable data sources on installed stocks, configurations, and the energy use characteristics of IT devices and cooling/power systems for enabling more common and accurate technology representation across models.
- **Storage, increased chip specialization** - In close alignment with dedicated EU initiatives IPCEI-CIS may also take into consideration cutting-edge innovation in the area of energy efficient chip production processes to integrate next generation hardware packages into the multi- provider cloud-edge continuum. This may also be linked to quantum technology development and HPC.

Via the support of a first industrial deployment (FID) the integrated project also fosters the initial Roll-out of new and innovative green technologies for clean data processing activities along the cloud edge continuum across the EU.

3.3 Standardization

Formal standardization processes are not the main purpose of the IPCEI-CIS but must be taken into account on several levels. The IPCEI is pursuing disruptive solutions for current and future market requirements which could open successful developments under the R&D&I activities to lend itself as basis for standards. In addition, the IPCEI must make sure that its developments do not create barriers for market entry by using proprietary foundations. Norms and standards can ensure market penetration of new ideas as well as compatibility, interoperability and portability. Therefore, the following actions are of particular importance in the aspect of the generation of spill-over effects resulting from the IPCEI-CIS activities:

1. Assessing the extent of available and emerging standards and making them, if appropriate, the basis for the IPCEI developments. This includes stocktaking of existing or emerging standards for the building blocks of the IPCEI technology stack and aligning to the roadmap of Standard Setting Organizations (SSOs) like CEN/CENELEC and ETSI, where appropriate.
2. In case of the identification of gaps (issues that are not yet standardized) and the aforementioned disruptive technologies, the support to standardization activities when needed for instance through the development of implementations to be used as references. Such a support could include liaisons with relevant committees (SSOs) responsible for the drafting of standardization proposals. Areas for potential identification of gaps could include, e.g.: scalable, flexible and highly automated compute and container services and scalable interconnections in a Multi Provider Cloud-Edge Continuum.
3. Creating an environment where the open source results of IPCEI-CIS developments can be published according to common open source software licences. This ensures a solid basis for further developments and eases the way for adaptation by other sectors across the EU.

This process ensures a broad adaptability of the IPCEI-CIS results in other application contexts and their exposure exceeding the participating companies and Member States.

3.4 Cloud Edge Capabilities for federated Data Spaces and Services

A secure and efficient data sharing is essential for federated data spaces to exchange data seamlessly between academia, industries, private stakeholders and/or public organisations. The IPCEI-CIS will enable data spaces to create value and will set up the necessary infrastructure and services for public and private sectors to give access to their relevant data sets in the cloud-edge continuum.

The operationalization of data spaces with a growing number of data sources mainly depends on infrastructure and service capabilities along the entire value chain. Therefore, the IPCEI-CIS focuses on flexible and agile data processing capabilities. This is necessary to integrate all involved edge nodes in the Multi Provider Cloud-Edge Continuum. The IPCEI-CIS is targeting on the interconnection of flexible and scalable cloud-edge computing capabilities to ensure interoperability, bandwidth availability, ultra-low latency and dynamical load balancing for next generation green data processing solutions of tomorrow. Those solutions need to be deployed with highly automated compute and storage capabilities, such as requirements for data encryption, data anonymization, traceability and the governance of the data sharing. For future applications in data spaces, the aggregation and pre-processing of data is required to guarantee the necessary data quality.

Therefore, the IPCEI-CIS will provide the next generation of data processing capabilities to connect common EU data spaces to the Multi Provider Cloud-Edge Continuum. For instance, to ensure data ownership capabilities it will provide compliant next generation solutions for a secure and sustainable data storage, exchange, processing, and access. This will ultimately operationalize data spaces in the decentralized Multi-Provider Cloud-Edge Continuum developed by the IPCEI-CIS.