CODECO's Validation and Experimentation Challenges

Field	Details
1. **Name of Challenge**	CODECO secure connectivity
2. **Partners**	UC3M/TID
3. **Submission Specifications**	The submission is structured around two main focal actions, each associated with a set of technical activities: **1. Performance Evaluation of the Secure Connectivity Component:** Evaluate the performance of the secure connectivity component in terms of installation and virtual network setup times, under varying cluster conditions. *Associated technical activities:* • Measure the installation time of the secure connectivity component, including the creation of the L2 overlay, while varying the number of nodes in the Kubernetes cluster. For each configuration, a significant number of samples must be collected and results visualized graphically to observe trends as the cluster size increases. • After installation, simulate the creation of virtual networks of type VLINK (emulating SWM-generated requests) and measure the time required for their provisioning. Tests should be conducted with varying numbers of cluster nodes, and under conditions with and without pre-existing virtual networks, to evaluate the impact on creation time.

	2. Implementation of a Passive Monitoring Feature: Extend the secure connectivity component with a passive monitoring capability to collect traffic metrics from the overlay network and assess application behaviour. *Context:* The overlay network is implemented as an L2 topology using VxLAN tunnels established between Open vSwitch (OVS) instances running as pods on each Kubernetes node. The creation and management of VLINK virtual networks over this overlay is coordinated by an SDN controller, specifically ONOS. *Associated technical activities:* Design and integrate a passive monitoring mechanism capable of capturing traffic metrics from the OVS instances involved in the overlay. The goal is to enable visibility into how applications use the overlay network, assess compliance with declared traffic requirements, and detect potential misuse or inefficiencies. Two possible implementation approaches are proposed: • Internal instrumentation, by modifying or extending the existing OVS pods or ONOS controller to expose relevant traffic metrics. • External observation, by deploying monitoring agents that collect traffic statistics using interfaces such as OpenFlow, sFlow, or Prometheus exporters. This dual-track challenge allows participants to choose between quantitative performance analysis and the development of enhanced monitoring features, depending on their interests and expertise.
4. Plataforms to be used	The proposed setup consists of using a virtual machine (VM) to deploy virtualized Kubernetes clusters via the *kind* tool. Each cluster will be configured with a different

	number of nodes. On top of each deployment, the secure connectivity component will be installed independently from the rest of the CODECO framework, with the objective of performing validation and testing procedures. Configuration files, scripts, and documentation will be provided to support these tasks. To prevent compatibility issues with preferred virtualization platforms (e.g., VirtualBox, virt-manager, VMware, AWS), no VM image will be distributed. The VM must meet the following minimum specifications: 8 vCPUs, 16 GB of RAM, 50 GB of storage, and an x86_64 (AMD) processor architecture. A backup of the submission should be uploaded via the application form.