ESTIMED (STF 685) Hackathon #1

Objectives

October 28th - 30th 2025, Remote

Track	*Description*	*Mandatory*
1	**Bring innovative use cases that address specific problems and challenges using oneM2M and MEC capabilities (IoT and Edge Computing).** The identification of the use cases shall follow a structured format that makes the problem clear and highlights how and why the interworking between oneM2M and MEC is important. The description shall include: • **Domain and Context**: specify the application domain (e.g., smart cities, industrial automation, maritime, healthcare, metaverse, smart home, digital twins, etc.) and explain the current challenges of that domain. • **Problem Statement**: identify a specific problem and challenges to be solved and why it is important in terms of safety, efficiency, sustainability, costs reduction, etc. • **Use Case Scenario**: to present a narrative describing how the system works from the perspective of the end-users or stakeholders (e.g., a connected ship approaching a port shall avoid collisions in real time, requiring local data processing at the edge). • **Actors and Stakeholders**: to identify end-users as well as physical and digital systems involved (e.g., IoT devices, vehicles, robots, sensors, platforms, cloud services, etc.). • **Expected Benefits**: to identify concrete/tangible benefits of solving the problem (e.g., improved safety, improved operational efficiency, costs reduction, energy savings, etc.). • **User Requirements**: based on the actors and stakeholders, clearly identify the end-users needs by describing what they expect from the proposed solution/system expressed in user language, without technical details.	**Yes**

Co-funded by the European Union
Co-funded by EFTA

2	**Provide high level architecture of the proposed solution by explaining how combining oneM2M and MEC is addressing the identified challenges.** As soon as the use case is identified, the participants shall propose a high-level system architecture that illustrates how oneM2M and MEC together address the identified challenges. This description should cover the following aspects: • **Overall Architecture**: functional diagram showing the main layers and components (e.g., devices, edge nodes, platforms, applications, etc.), indicating where oneM2M and MEC components are deployed. • **System Requirements**: based on the user requirements, a comprehensive set of functional/non-functional system requirements shall be derived covering aspects such as performance, scalability, interoperability, security, reliability, latency, etc. • **oneM2M Components**: to describe which nodes are used (e.g., IN-CSE in cloud, MN-CSE at edge, ASN/ADN at devices, etc.), how devices and applications register and interact via oneM2M, and which Common Service Functions (CSFs) are used (e.g., data management, device management, security, semantic discovery, etc.). • **MEC Components**: to describe which MEC functions and building blocks are leveraged (e.g., MEC platform, MEC applications, MEC orchestrator, etc.), which MEC APIs are used, and how MEC hosts real-time applications (e.g., Federated Learning, AI analytics, Swarm Computing, etc.). • **oneM2M/MEC Interworking**: to describe how MEC applications consume or expose oneM2M services, how oneM2M data flows are directed to the MEC applications for low-latency processing, and what deployment options are used (e.g., A, B, C or D). • **Data Management**: to describe where time-sensitive data is processed, where a persistent storage and global coordination happens, and how data and service continuity are ensured when devices/users/assets move across zones (e.g., handover). • **Security and Reliability**: to describe how security is ensured (e.g., authentication, authorization, secure APIs, etc.), and how the reliability is managed at edge/cloud level. • **Impact**: to explain and highlight (from technical point of view) how the proposed architecture solves the identified problem/challenge (e.g., by placing MN-CSE on MEC nodes, collision avoidance algorithms can be executed quickly, ensuring safety during maneuvering operations).	**Yes**

Co-funded by the European Union
Co-funded by EFTA

3	**Develop a prototype of a MEC or oneM2M application exploiting existing oneM2M/MEC implementations and considering available oneM2M/MEC configurations (either in a form of a technical documentation or a real prototype).** In order to support the prototype development activities, the ESTIMED project provides the participants with all the required materials and tools (accessible through the project Git repository: (https://labs.etsi.org/rep/estimed/wp6/hackathons/hackathon-1.git) including: • **Tutorials**: MEC Tech Series, ETSI MEC Sandbox, step-by-step guidelines for developing a MEC application (sessions and network scenarios), oneM2M tutorials; • **User Guides**: ETSI MEC Sandbox deployment, procedure for developing a MEC application and test it against ETSI MEC Sandbox, practical examples, oneM2M guidelines. • **Proofs of Concept**: skeletons and tools for developing single or combined oneM2M and MEC applications. The participants are requested to submit (public Git repository) all produced material in the same format in order to facilitate its evaluation as follows: • **Project/Results Presentation**: MS PowerPoint. • A **hackster.io** project that is a clear guide on building a prototype solution. It includes: o Description of the issue and how the prototype solution addresses it. o An explanation of the oneM2M and MEC features used in the solution. o A description of devices, applications used (oneM2M platform, MEC framework, device simulators, etc.) • **A public repository to release the source codes**.	**Optional** **(Best Effort)**

Co-funded by the European Union

Co-funded by EFTA

Co-funded by the
European Union