MEC standards overview and cybersecurity perspective

Dario Sabella

VP at xFlow Research, ETSI MEC Chair

Athens (Greece), 10/12/2024

ETSI MEC: Enabling *Edge* through *Standardization*

Foundation for Edge Computing – Fully standardized solution to enable applications in distributed cloud created by ETSI MEC + 3GPP

Watch the new video on MEC

https://www.youtube.com/watch?v=crnPWql-0oo

Application Life Cycle Management

RESTful based APIs for Runtime Application Services

3GPP A GLOBAL INITIATIVE · WiFi · broadband forum

ETSI: The Standards People
producing globally applicable standards for ICT-enabled systems

ETSI ISG MEC

ISG: Industry Specification Group
open to all of industry, regardless of ETSI membership and focused on all industry needs

MEC: Multi-access Edge Computing
Cloud Computing at the Edge of the network.

ETSI MEC The Standards People

ETSI NFV The Standards People

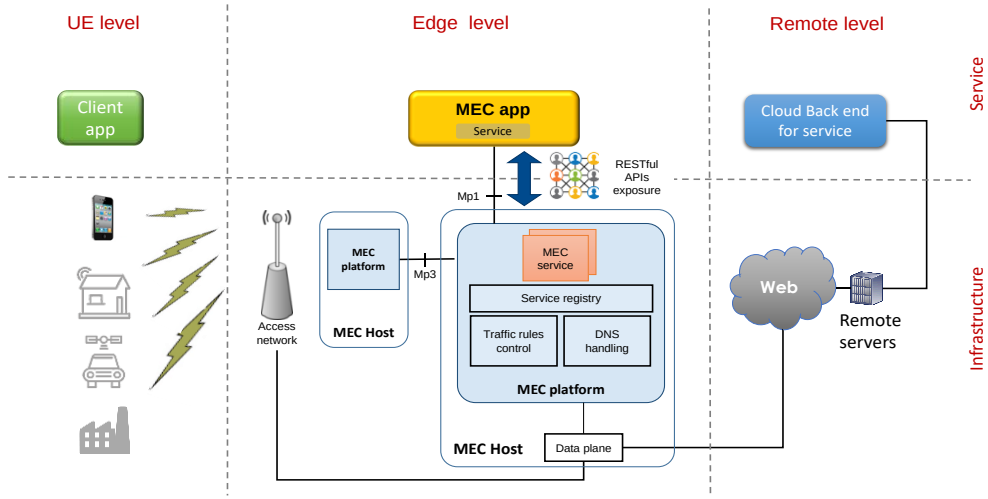
MEC Application Development Community
Interaction & Information Exposure

- **Continuously growing MEC membership:** 124 (updated Dec 2022); e.g. in June 2021 it was 114
- **Diverse ecosystem:** Operators - Technology Providers - IT players - Application developers - Startups - …

Renewed webpage: **ISG MEC Leadership Team, LS officers for Vertical Industries** and **MEC Support Team:** https://portal.etsi.org/TB-SiteMap/MEC/MEC-Leaders-and-Support-Team

ETSI MEC – Foundation for Edge Computing

MEC offers to application developers and content providers cloud-computing capabilities and an IT service environment at the edge of the network



Basic principles:

- *Open standard* → allowing multiple implementations and ensuring interoperability
- MEC exploiting ETSI *NFV framework* and definitions → enabling MEC in NFV deployments
- Alignment with *3GPP* based on fruitful collaboration of common member companies → enabling MEC in 5G
- Access-agnostic nature (as per MEC acronym - Multi-access Edge Computing) → enabling other accesses
- Addressing the needs of a wide ecosystem → enable multiple verticals (e.g. automotive), federations

MEC is focused on *existential* questions of **applications "on the edge"**

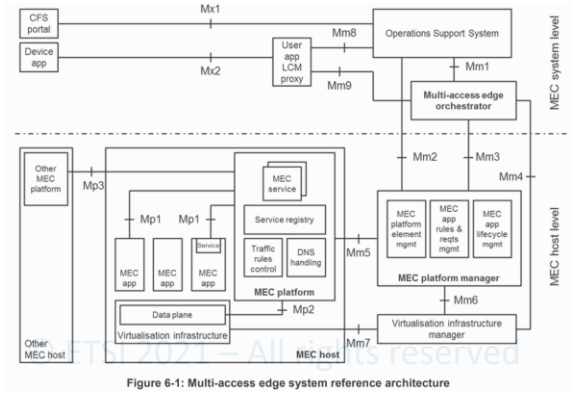
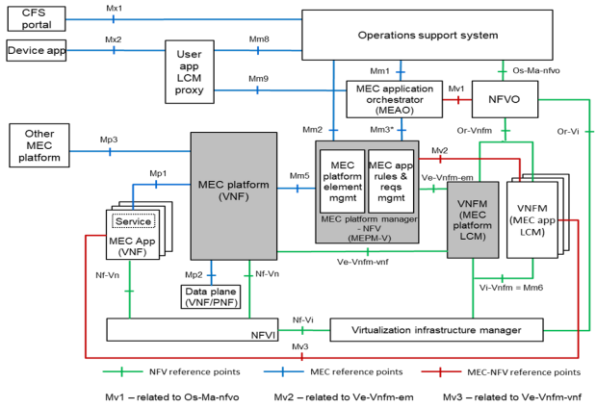
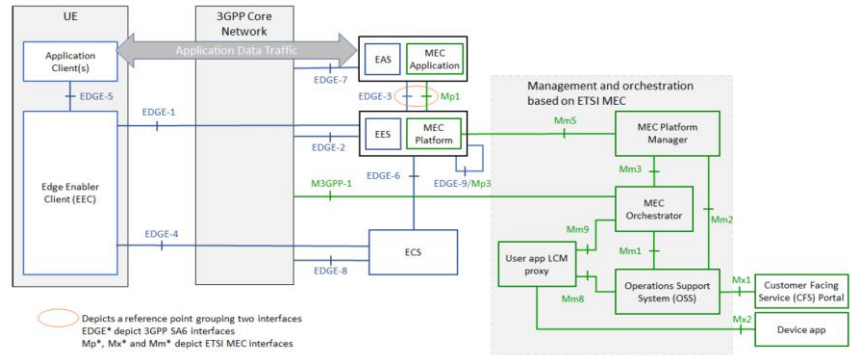


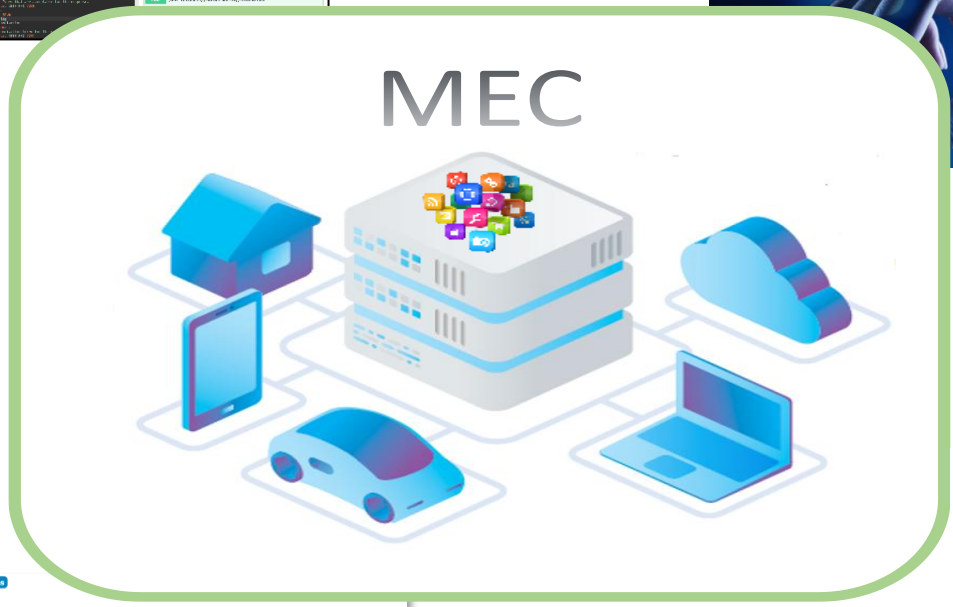
Figure 6-1: Multi-access edge system reference architecture

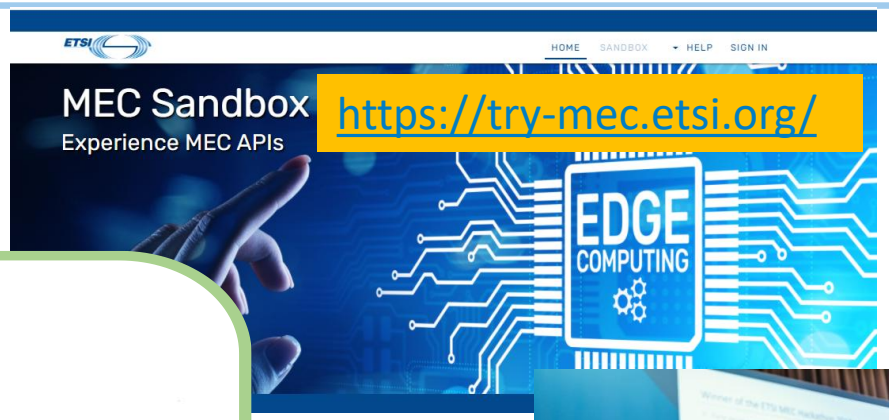




ETSI ISG MEC DECODE Working Group:
MEC Deployment and Ecosystem engagement activities

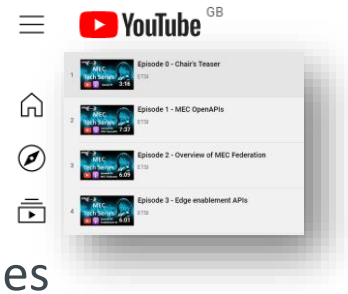
- OpenAPI representations: ETSI Forge
- Testing and Conformance
- MEC Ecosystem wiki
- PoCs (proof-of-concepts)
- MDTs (MEC Deployment Trials)
- MEC Sandbox
- Collaborations: CAMARA, STF
- Hackathons
- Plugtests
- MEC Tech Series

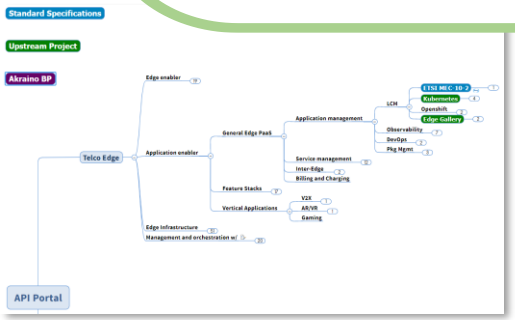




ETSI/LF Edge/OCP
Edge AI Hackathon 2023

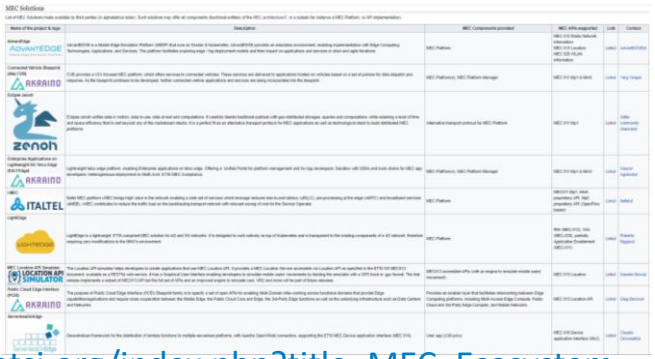
18 Oct 2023, San Jose, California
https://www.opencompute.org/blog/2023-ocp-global-summit-hackathon-was-amazing





https://apiportal.akraino.org/apimap.html

1 - 15 Oct 2021
NFV&MEC IOP
Plugtests 2021



https://mecwiki.etsi.org/index.php?title=MEC_Ecosystem

MEC Standard work: from Phase 1 to Phase 4

- Key overall specification
  - Technical Requirements (MEC 002)
  - Framework and Ref. Archit. (MEC 003)
  - MEC PoC Process (MEC-IEG 005)
  - API Framework (MEC 009)
- IaaS Management APIs
  - Platform mgmt. (MEC 010-1)
  - Application mgmt. (MEC 010-2)
  - Device-triggered LCM operations (MEC 016)
- PaaS Service Exposure
  - Required Platform Svcs / App. Enablement (MEC 011)
  - Service APIs (MEC 012, 013, 014, 015)
- Key Studies for Future Work
  - Study on MEC in NFV (MEC 017)
  - Study on Mobility Support (MEC 018)

- Evolution of Phase 1 and closing open items
  - Application Mobility (MEC 021)
  - Lawful Intercept (MEC 026)
- Addressing key Industry Segments
  - V2X (MEC 022 – published; MEC 030)
  - Industrial Automation, VR/AR
- Key use-cases and new requirement
  - Network Slicing (MEC 024)
  - Container Support (MEC 027)
- Normative work for integration with NFV
  - Incorporate in v2 of existing specifications as needed
- From "Mobile" to "Multi-Access"
  - Wi-Fi (MEC 028)
  - Fixed Access (MEC 029)
- MEC integration in 5G networks (MEC 031)
- Developer community engagement
  - API publication through ETSI Forge (overleaf)
  - Hackathons, MEC Delpoyment Trials
- Testing and Compliance (MEC-DEC 025; multipart spec MEC-DEC 032-x)

- Full Phase 3 work (with some pre-Phase 4).
- MEC as heterogeneous clouds
  - Expanding traditional cloud and NFV LCM approaches
  - Inter-MEC systems and MEC-Cloud systems coordination: "MEC Federation" (MEC 035, MEC040)
  - Mobile/intermittently connected and resource constrained devices (MEC 036), MEC IoT API (MEC 033)
- MEC Security (GR MEC 041)
- MEC deployments, e.g. in Park enterprises (MEC 038)
- MEC Application Slices (MEC 044)
- Continuing emphasis on enabling developers
  - App Package Format and Descriptor (MEC 037)
  - API Serialization
  - MEC Sandbox development
  - Testing and compliance
- Continue to define services that meet industry demand (e.g., Abstracted Network Info Exposure, MEC 043)
- Maintain and enhance existing APIs (MEC 013)

- Evolution of Phase 3 and closing open items, including maintenance and enhance existing APIs
- Addressing key Industry Segments
  - Listen to verticals via Edge Discovery Days
  - Abstracted Network Info Exposure MEC 043
  - Distributed Edge Network MEC 047
  - Exploiting Edge Computing Resources MEC 059
- Key use-cases, requirements & arch
  - MEC 002, MEC 003
- Normative work on MEC Security
  - MEC architecture (MEC 003), (API GW for Client Apps (MEC 060), Support for Security Monitoring and Management (MEC 062)
- Continuing emphasis on enabling developers
  - Testing and compliance
  - API-driven MEC Sandbox and Edge Native Connector activities (STF678)
- Collaboration with open-source communities (e.g., TeraFlowSDN, OpenCAPIF, CAMARA)
- STF 685 ESTIMED: Enabling Standardized IoT deployments in MEC Environments for advanced systems (OneM2M & SmartM2M)
  - 9 GR/GS, 4 PoC, Testing
- AI/ML in MEC (MEC 061)

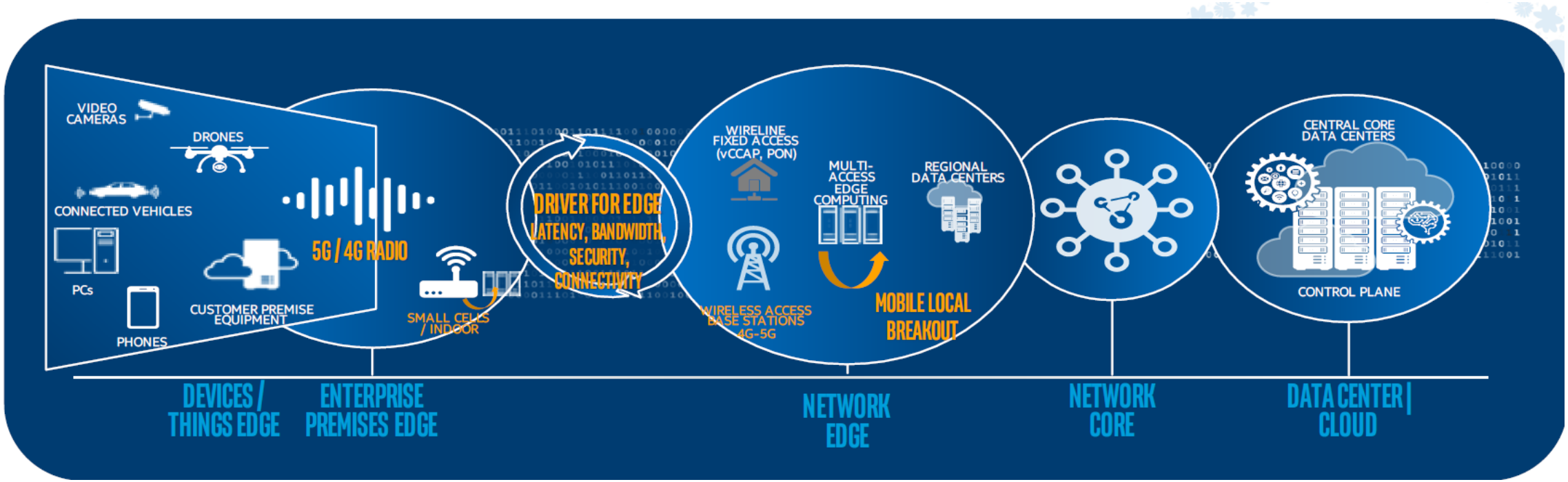
2015 ETSI MEC phase 1 (Completed) → 2018 ETSI MEC phase 2 (Completed) → 2021 ETSI MEC phase 3 (Completed) → 2024 ETSI MEC phase 4 (Started)

MEC Cybersecurity perspective

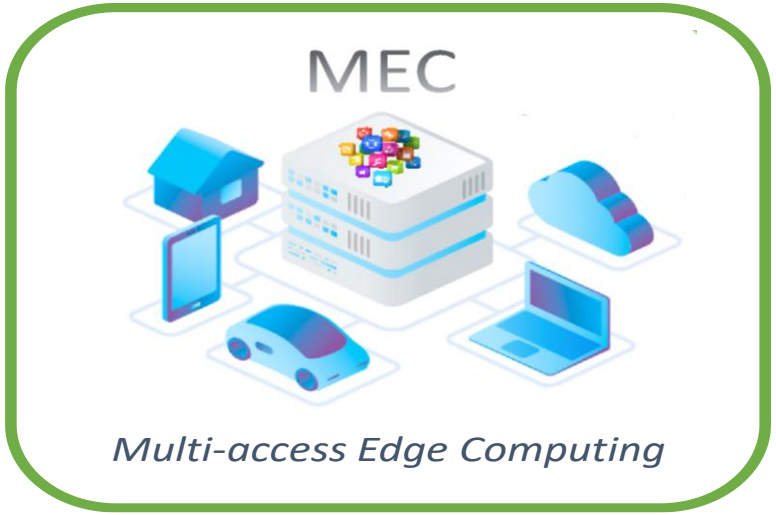
Edge Security – an end-to-end perspective

- Diverse Ecosystem and stakeholders
- Multiple deployment options and KPIs
- Open market and new business models

In this heterogeneous context, security, privacy and trust are key topics for the edge



MEC security: status of standards support and future evolutions



- **MEC scenarios** are characterized by a complex multi-vendor, multi-supplier, multi-set of equipment including both HW and SW devices. Given this overall level of **system heterogeneity**, areas of security, trust, and privacy are key topics for the edge environments.
- In that perspective, MEC stakeholders should pay attention to the vulnerability and integrity of any third-party elements, and a truly **end-to-end approach to MEC security** needs to consider not only the current standards in ETSI ISG MEC, but also the other available standards that can be applicable to the MEC environment.

- **ETSI white paper**, authored by many experts (in the domain of edge computing, security and involved in various standard bodies), provides an overview of **ETSI MEC standards** and current support for security, which is also complemented by a description of other relevant standards in the domain (e.g. **ETSI TC CYBER**, **ETSI ISG NFV**, **3GPP SA3**) and **cybersecurity regulation** potentially applicable to edge computing.
- https://www.etsi.org/newsroom/press-releases/2123-2022-09-etsi-publishes-a-new-white-paper-on-multi-access-edge-computing-security

Second edition published Sept 2022

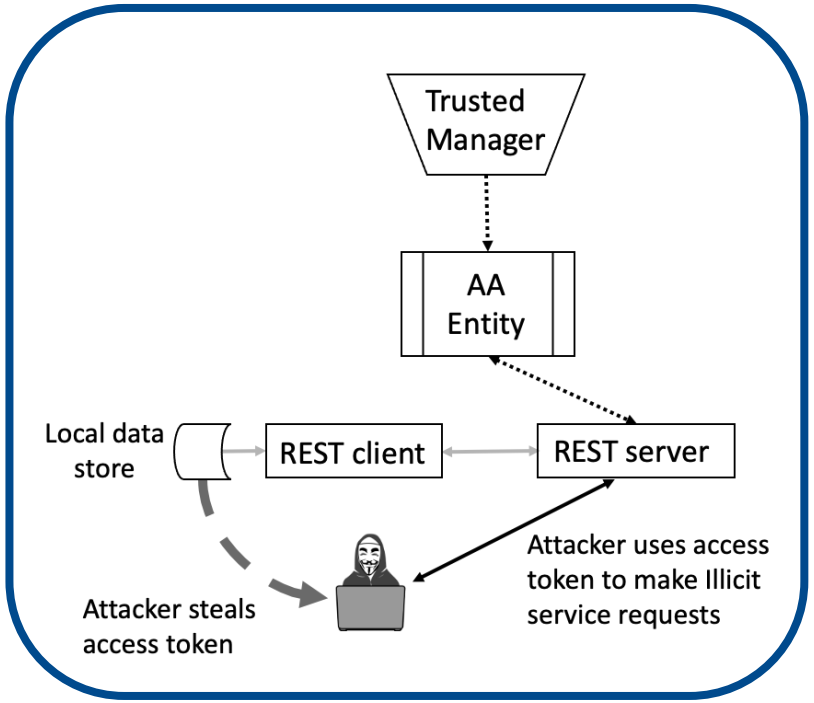
MEC Phase 3: Study on MEC security

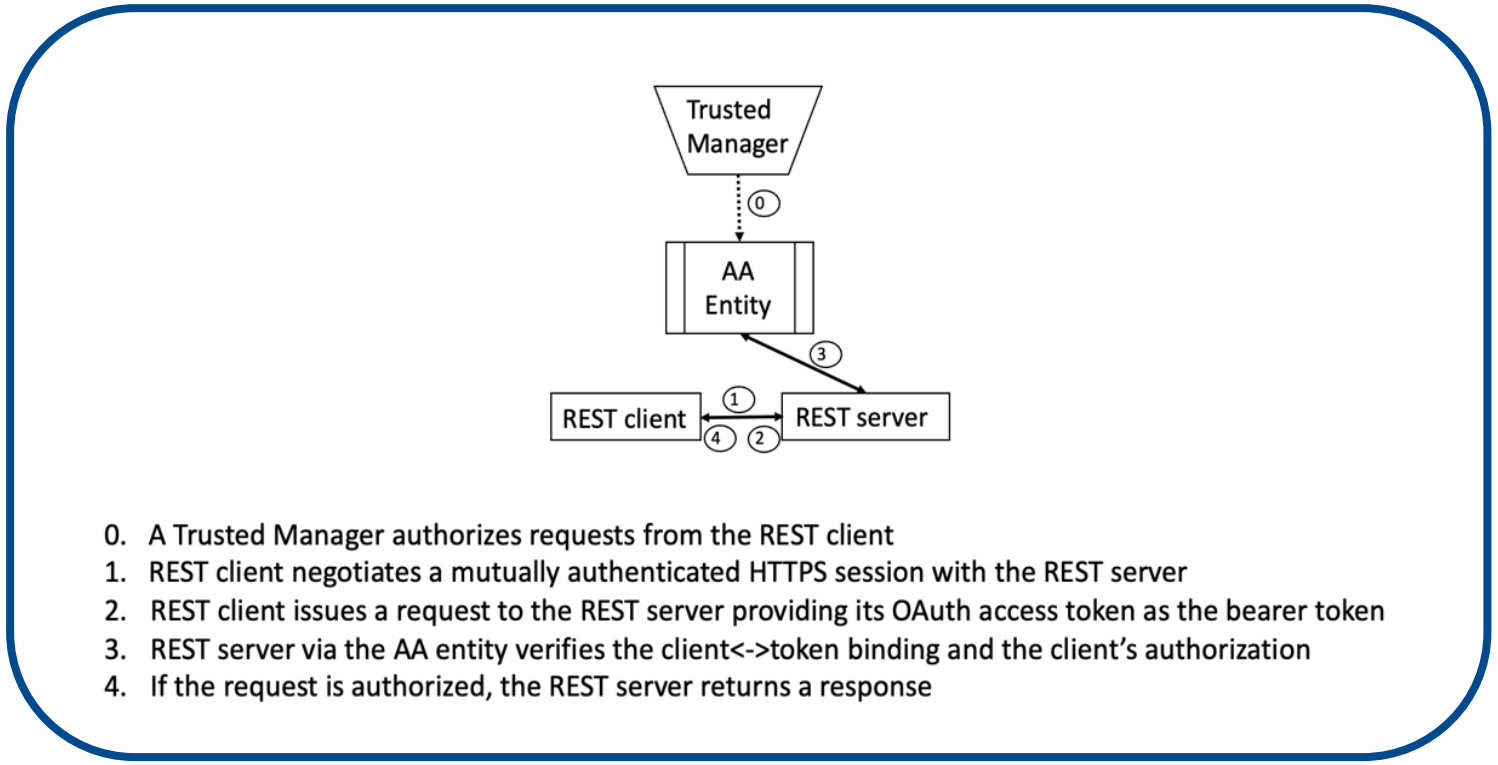
- ETSI GR MEC 041
- https://www.etsi.org/deliver/etsi_gr/MEC/001_099/041/03.01.01_60/gr_MEC041v030101p.pdf

- The document outlines security topics and paradigms that apply to MEC deployments across the realms of application/platform security and zero-trust architecture.
- The document considers prior work of other standards bodies and industry associations.
- It identifies gaps in ETSI ISG MEC specifications and provides recommendations for new normative work.

MEC Phase 3: Study on MEC security

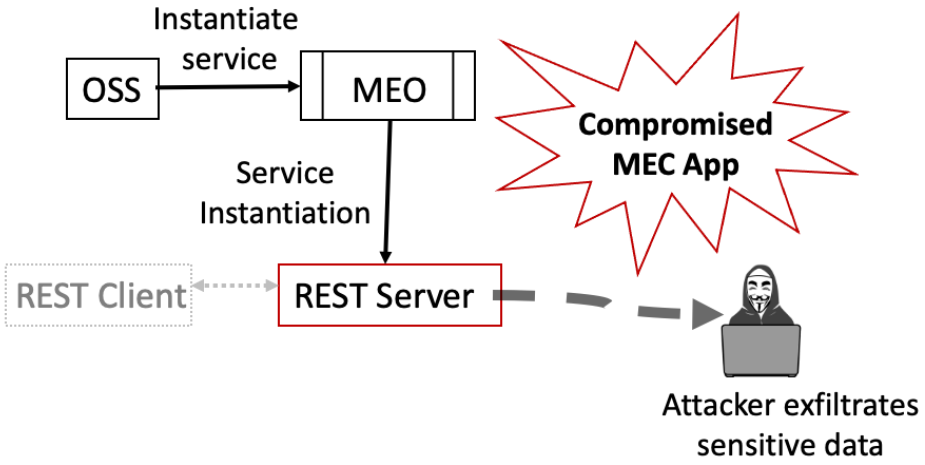
- Examples of studied Key Issues:
  - **Key issue #1**: Stolen MEC App access tokens
  - **Solution proposal #1**: Adopt OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens

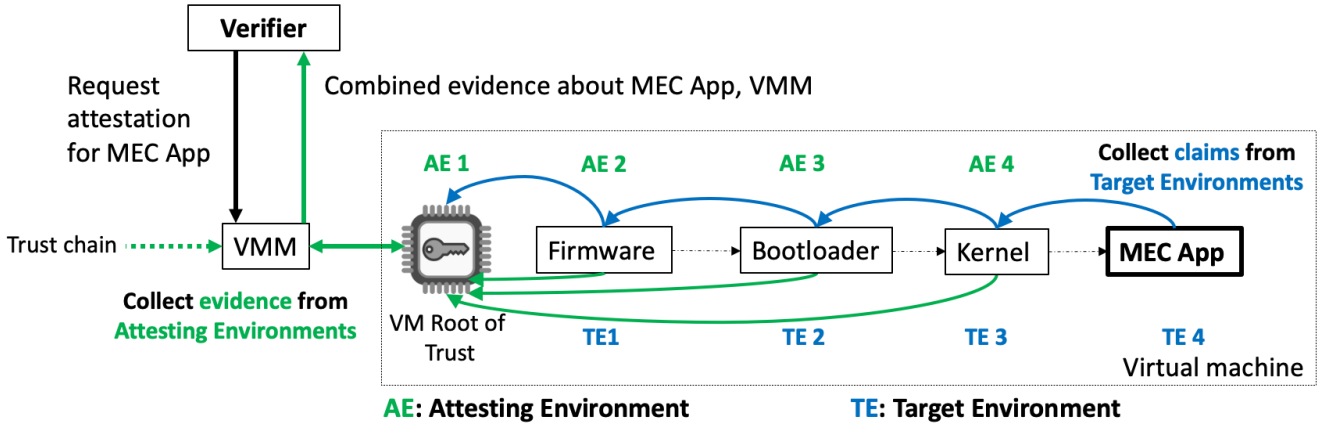




MEC Phase 3: Study on MEC security

- Examples of studied Key Issues:
  - **Key issue #3**: Compromised MEC applications, asset theft
  - **Solution proposal #1**: Verify provenance of MEC applications through cryptographic attestations





MEC Phase 3: Study on MEC security

- Examples of studied Key Issues:
  - **Key issue #7**: MEC App anomalous behaviour
  - **Solution proposal #1**: Security Monitoring and Management for MEC

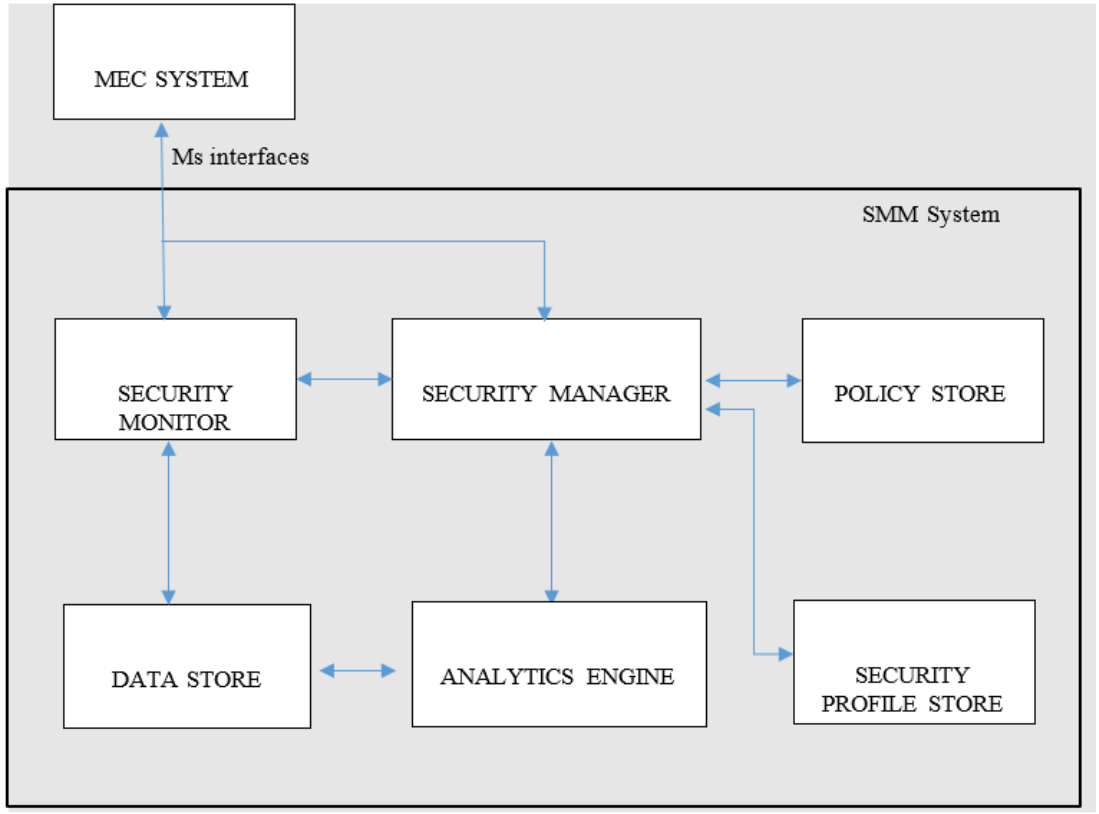


Figure 5.7.2.1-1: MEC System interfaced to an SMM System Functional Architecture

an SMM system interfacing to a MEC system could include the following Functional Elements:

- Security Monitor
- Data Store
- Analytics Engine
- Security Manager
- Policy Store
- Security Profile Store

MEC Phase 4 work on security

MEC 009 – General principles, patterns and common aspects of MEC Service APIs

MEC 011 – Edge Platform Application Enablement

MEC 016 – Device application interface

This work item focuses on device app authorization aspects, such as clarification of authorization process; selection of authorization token type; guidance on how to obtain client certificates if needed. Alignment with relevant 3GPP CAPIF UE-related security solutions will be sought.

MEC 060 – API Gateway for Client Applications

This work item specifies the security related interaction between the API Gateway and Client Applications. This includes obtaining authorization to access the services (via the client-facing interfaces) provided by the MEC Applications, revoking this authorization upon certain conditions (e.g. overflow/DOS). This work item specifies, if supported, the interactions between the API Gateway and MEC management for obtaining security-related configuration (if any) for MEC Applications.

MEC 062 – Support for Security Monitoring and Management

This work item specifies the implementation of MEC support for Security Management and Monitoring (SMM) feature. It will describe the information flows, will list security-related data to be collected, and as applicable, will specify the necessary data model and data format. This work item will provide guidelines to enable integration into existing security automation tools. This work item will also provide MEC SMM related informative descriptions on the use of security profiles, directives, policies, and the functionality of collection, distribution, and storage of security data.

Looking forward on MEC security…

Future security challenges on edge computing will be naturally associated to the evolution of the related infrastructural technologies, cloud and networking

Some technology trends:

- Cloud-native design and serverless approaches, also in hybrid clouds and NFV
- in-network computing (seamless integration of computing and networking)
- integration of acceleration mechanisms both in computing and network forwarding
- pervasiveness of AI and its strong dependency on dependable data flows
- … and of course, the evolution of networks towards 6G systems.

Thank you for your attention

Dario Sabella

VP at xFlow Research, ETSI MEC Chair