ETSI White Paper No. #46

MEC security; Status of standards support and future evolutions

2nd edition – September 2022

ISBN No. **979109262041**

Authors:

Dario Sabella, Alex Reznik, Kamal Ranjan Nayak, Diego Lopez, Fei Li, Ulrich Kleber, Alex Leadbeater, Kishen Maloor, Sheeba Backia Mary Baskaran, Luca Cominardi, Cristina Costa, Fabrizio Granelli, Vangelis Gazis, Francois Ennesser, Xi Gu, Faraz Naim, Dan Druta

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

Authors

Dario Sabella (Intel, ETSI ISG MEC chair)	*Kishen Maloor (Intel, ETSI ISG MEC delegate)*
Alex Reznik (HPE, ETSI ISG MEC delegate)	*Sheeba Backia Mary Baskaran (Motorola Mobility, ETSI ISG MEC delegate)*
Kamal Ranjan Nayak (iLink, ETSI ISG MEC delegate)	*Luca Cominardi (Adlink, ETSI ISG MEC delegate)*
Diego Lopez (Telefonica, ETSI ISG NFV NOC chair, ETSI ISG ZSM chair)	*Cristina Costa (FBK, ETSI ISG MEC delegate)*
Fei Li (Huawei, ETSI ISG MEC delegate)	*Fabrizio Granelli (CNIT, ETSI ISG MEC delegate)*
Ulrich Kleber (Huawei, ETSI ISG MEC delegate and NFV EVE vice-chair)	*Vangelis Gazis (Huawei, ETSI TC CYBER delegate)*
Alex Leadbeater (BT, ETSI TC CYBER chair, ETSI ISG NFV SEC chair and 3GPP SA3-LI Chair)	*Francois Ennesser (Huawei, ETSI TC CYBER delegate)*
Xi Gu (ZTE, ETSI ISG MEC delegate)	*Faraz Naim (Accenture, ETSI ISG MEC delegate)*
Dan Druta (AT&T, ETSI ISG MEC delegate, W3C co-chair of Web & Networks Interest Group)	

Contents

Executive Summary

The present White Paper will focus on MEC (Multi-access Edge Computing) technologies and intends to explore security-related use cases and requirements with the aim of identifying aspects of security where the nature of edge computing results in insufficient industry approaches to cloud security.

Edge computing environments are by nature characterized by a complex multi-vendor, multi-supplier, multi-stakeholder ecosystem of equipment including both HW and SW devices. Given this overall level of system heterogeneity, the areas of security, trust, and privacy are key topics for the edge environments. Finally, the advent of edge cloud federations and the presence of (far) edge devices, e.g., in Internet-of-Things environments, requires tackling MEC security with an end-to-end (E2E) approach by leveraging existing standards relevant in the area, as carefully selected to be applicable in edge computing systems.

In this heterogeneous scenario, talking about end-to-end MEC security implies considering the impact on the elements coming from all stakeholders involved in the system. In that perspective, MEC 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 MEC environment. In this perspective, the White Paper will provide 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. Other than a description of security use cases and requirements for MEC, an analysis of security threats related to MEC federation is provided, as standardization work in ETSI MEC (but also in 3GPP) is expected to consider this GSMA work and put necessary measures in place to enable the actual deployment of the MEC Federation, which is very critical for operators and service providers. Finally, a general perspective of future evolutions and standard directions on MEC security will complete the work.

This 2nd edition of the MEC Security White Paper is then a must-read for all ecosystem stakeholders as the adoption of edge computing technologies introduces a need for infrastructure owners and application/content providers to guarantee a level of security on the usage of edge computing assets in order to meet customer demands. Providing the needed clarifications in this White Paper, as the very first initiative in this domain, is a step forward for the alignment of the edge ecosystem and a means to further encourage the adoption of MEC technologies.

1 Introduction

Multi-access Edge Computing (MEC) offers application developers and content providers cloud-computing capabilities and an IT service environment at the edge of the network [ref. ETSI-MEC]. This technology enables an open market and new business models, including the possibility to serve multiple use cases and applications. Edge computing environments are also characterized by a diverse ecosystem of market players ranging from infrastructure owners to service providers and system integrators to application developers. In this multi-stakeholder ecosystem, edge computing infrastructure, MEC platforms and applications in most deployments are provided by different entities. Telcos established partnerships with public cloud providers and use some of their components in their edge cloud. In addition to that, the heterogeneous nature of the edge environments (RAN and core functions running along with third party applications with a mix of container-based and VM based deployments) makes these configurations prone to zero-day vulnerabilities. Lastly, the edge components are deployed in physically isolated and insecure locations such as cell sites or isolated central office buildings more vulnerable to physical attacks than centralized data centers.

All these factors call for key security measures and considerations such as:

- Implementing Zero-Trust strategies - Zero Trust is a paradigm shift towards security and eliminates the implicit trust security, access-control, list-based filtering with stronger authentication, authorization to ensure “least access” policies.
- Securing perimeter- Securing access to edge computing resources leveraging encrypted tunnels and firewalls
- Securing applications - Edge computing devices run apps that need to be secured beyond the network layer
- Vulnerability and Patch management: The continued monitoring and discovery of known and unknown vulnerabilities as well as automated patching to keep devices updated and reduce attack surfaces.

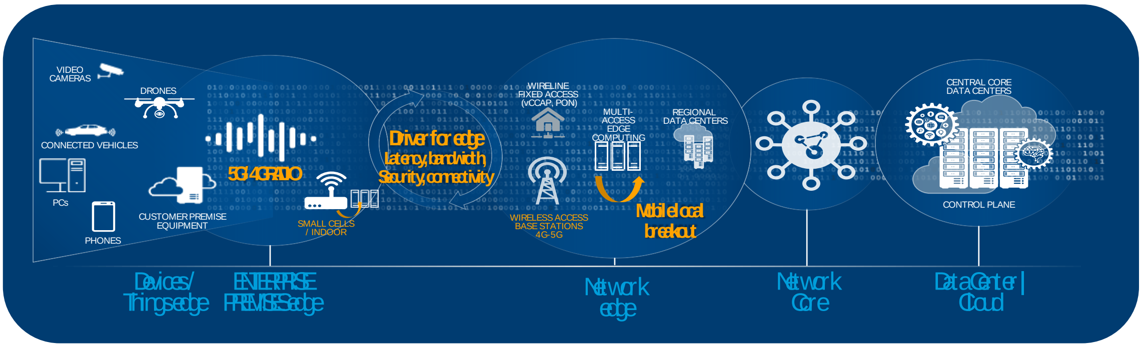

Figure 1: Examples of deployments in edge computing environments

In this context, as well as the way this technology is deployed on virtualized infrastructures, there are multiple options to stakeholders with each deployment option being characterized by different KPIs. Such options may be more suitable for certain applications and use cases, although possibly accompanied with different security challenges. Given this overall level of system heterogeneity, the areas of security, trust, and privacy are key topics for the edge environments. Finally, the advent of edge cloud federations and the presence of (far) edge devices, e.g. in Internet-of-Things environments, requires tackling MEC security with an end-to-end (E2E) approach by leveraging existing standards relevant in the area, as carefully selected to be applicable in edge computing systems.

The approach of this White Paper is to present a comprehensive, and well targeted, selection of standards relevant in the context of MEC security. The starting point is of course a reference to ETSI ISG MEC (Multi-access Edge Computing), which is itself based on ETSI NFV (Network Function Virtualization) framework and architectural definitions and builds upon the work done by ETSI TC CYBER relevant for edge clouds and MEC security issues.

The White Paper is organized as follows: Section 2 will cover MEC security use cases and requirements, Section 3 will provide an overview of the main standards available in the space to address these use cases, Section 4 will contain a brief overview of security regulations relevant to MEC, and finally Section 5 will conclude the White Paper with some considerations on future evolutions for the MEC security support.

2 MEC security use cases and requirements

Edge computing environments are by nature characterized by a complex multi-vendor, multi-supplier, multi-stakeholder ecosystem of equipment including both HW and SW devices. In these distributed systems, one cannot assume to have a central entity that implements system-wide security assurances or would accept full liability if things go wrong. Besides this, the multi-party nature of edge environments requires mechanisms to assess the trust each party can put on the other, in a way that considers adequately the dynamic nature of the environment, especially in events related to lifecycle management, such as deployment or migration. Additionally, while MEC deployments may include edge-instantiated copies of core 3GPP or similar network functions, the more exposed nature of MEC deployments away from core data centers exposes both the virtual MEC functions and the management links to additional threats. Thus, in an E2E approach and by looking at the MEC architecture, many specific use cases related to MEC may need special attention from a security perspective.

2.1 MEC (Multi-access Edge Computing) reference scenario

The MEC initiative is an Industry Specification Group (ISG) within ETSI. The purpose of the ISG is to create a standardized, open environment that will allow the efficient and seamless integration of applications from vendors, service providers, and third parties across multi-vendor MEC-compliant platforms. The ISG MEC published a comprehensive set of specifications, ranging from MEC architecture [ref. MEC-003] to a set of APIs (both IaaS Management APIs for the application LCM operations, and PaaS Service Exposure APIs). In particular, the figure 2 below shows how the MEC service APIs can expose useful information for Application Developers (for more details see the Application Enablement API [ref. MEC-011]). The ETSI MEC standard defines only some exemplary Service APIs as requested by the industry (e.g.: Radio Network Information API [ref. MEC-012], Location API [ref, MEC-013], etc., …) or relevant from some particular vertical market segments (e.g. V2X API [ref. MEC-030] for the automotive domain). In addition to that, also new APIs (compliant with the generic principles and guidelines for MEC service API design [ref. MEC-009]) can be added by third parties and exposed to applications, thus enabling a myriad of new use cases and business models across the ecosystem. This powerful and open mechanism has of course also implications in terms of security, as multiple stakeholders are supposed to own and manage different portion of the overall software stack.

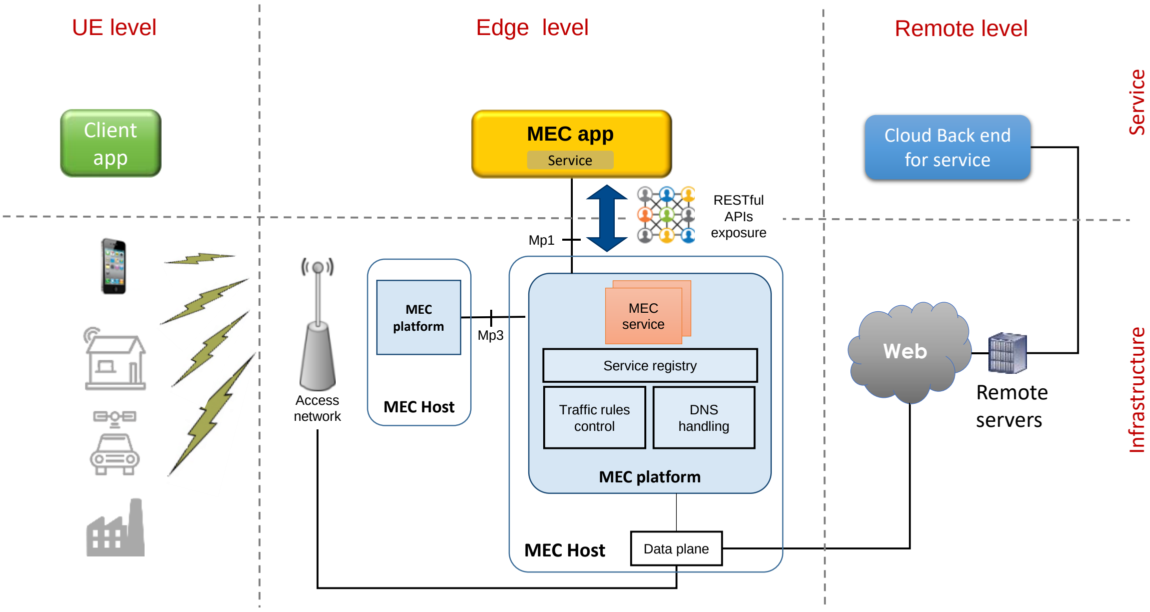

Figure 2: MEC applications, interaction and service exposure

Despite its access-agnostic nature (as MEC acronym stands for Multi-access Edge Computing), MEC has an essential role in the 5G infrastructure since Edge Computing can be an enabler for various 5G usage scenarios (i.e., eMBB, URLLC, mMTC). Besides enabling the deployment, lifecycle management, innovative applications, and services towards mobile subscribers, enterprises, and vertical segments, the MEC framework also provides services that support mobility and radio-related information.

Also, the 3GPP EDGEAPP architecture (defined in SA6) introduces Edge Computing elements, and a great degree of synergy exists between it and the ETSI ISG MEC. The ETSI ISG MEC architecture core lies in the MEC Platform and the MEC Applications, while for the 3GPP SA6 the core is represented by the Edge Enabler Server and the Edge Application. These functional entities carry a certain degree of alignment and complementarity that have been expressed in the Synergized Mobile Edge Cloud Architecture, where synergies between the architectures are exemplified.

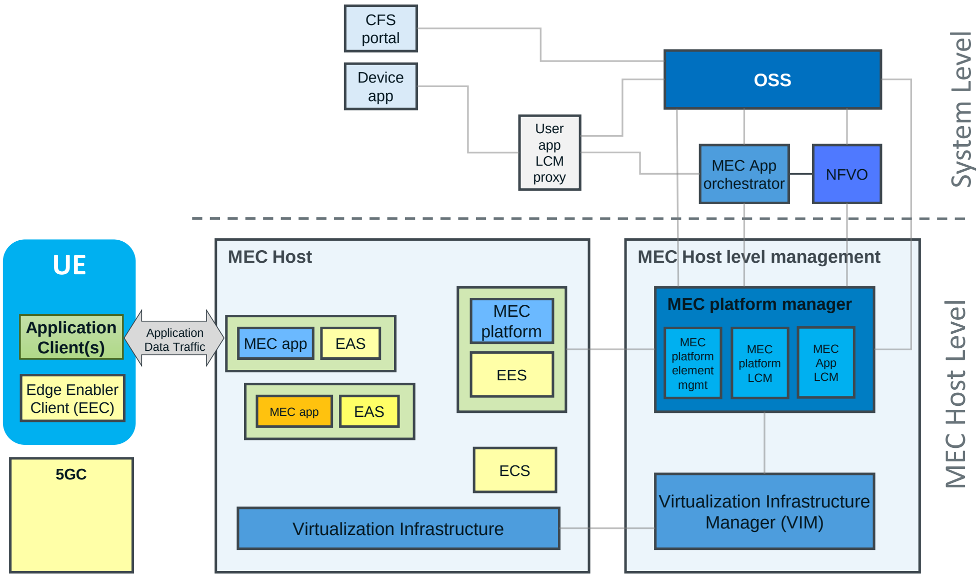

Figure 3: High-level overview of synergized MEC architecture in virtualized environments

More in detail, ETSI has recently published the GR MEC 031 [ref. MEC-031] that evaluates possible proposal solutions, identifies gaps, and produces recommendations for MEC integration into 3GPP 5G system. From the 3GPP side, the TS 23.558 provides application layer architecture and related procedures for enabling edge applications over 3GPP networks [ref. TS23.558].

From the security point of view, the new functional elements introduced by the synergized architecture together with the introduction of third-party applications at the edge of the Radio Access Network (RAN) may considerably extend the surface attack.

2.2 Security use cases and requirements for MEC

The MEC paradigm enables new vertical businesses and services for consumers and enterprises. However, as a distributed cloud with nodes located in potentially poorly secured environments and likely running critical workload, it presents a set of unique security challenges. In this subclause we provide an overview of the threats landscape associated with MEC and requirements related to MEC security. Our work is based to a significant extent on the use cases as defined in ETSI GS MEC 002 [ref. MEC-002] and the ENISA '5G threat landscape' Report [ref. ENISA-5G].

MEC is designed to support various use cases such as video analytics, location services, Internet-of-Things (IoT), Augmented Reality (AR), optimized local content distribution, data catching, and more. The MEC system should provide a secure environment for running services for various involved actors such as user, network operator, third-party application provider, application developer, content provider, and platform vendor. Based on ENISA 5G Threat Landscape, the potential threats related to MEC include:

(i) Abuse of assets, which mainly involves exploitation of software or hardware vulnerabilities leading to Zero-day exploits, software tampering and system execution hijack which can impact information integrity, service availability, etc.; furthermore, APIs serve as conduits that expose applications for third-party integration; as a consequence of that, also APIs are potentially susceptible to attacks like any other software.

(ii) Compromised supply chain, vendor, and service providers due to tampering of network product (configuration or source code), abuse on third parties' personnel access to MNO facilities and manipulation of network product updates can also result in service unavailability, information destruction and initial unauthorized access.

(iii) Unintentional damages that may occur due to misconfigured or poorly configured systems, inadequate designs, and erroneous use or administration of the network, system, and devices can potentially impact service availability and information integrity.

The threats pertaining to MEC can be common to most of the use cases, and the threat factors can be broadly categorized based on various areas of vulnerabilities related to Platform Integrity, Virtualization and Containerization, Physical security, Application-Programming Interfaces (APIs), and Regulatory issues.

Based on the type of virtualization and containerization used, the MEC system can be susceptible to a number of threats emerging from these technologies, e.g., possible contamination of shared hardware resources, abuse of privilege elevation of containers with higher levels of privileges, use of open-source APIs, etc. Vulnerabilities in the MEC virtualization platform can include compromise of the underlying system (FW, Bootloader, Host OS/Hypervisor), inadequate isolation of resources in OS/container layers and vulnerabilities specific to cloud technologies used in MEC implementation. Potential requirements to address inadequate isolation can include network segmentation, resource separation, data segregation, software and network attestation, etc. Improper hardening of MEC components can include presence of unrestricted reachability for services, unused software/functions/components, improper separation of traffic etc., Hardening requirements must ensure that all the default configurations (including OS software, firmware, and applications) are appropriately set and, going beyond, that these settings can be verified against a reference. Countermeasures such as filtering of packets heading for the target site under attacks, restriction of communication port used for DoS/DDoS attacks, and reduction or suspension of operation of target telecommunications facilities need to be considered. Software vulnerabilities in MEC applications can be used as an entry point to exploit other MEC components and internal interfaces which may result in unauthorized access to data, elevation of privileges and cloud intrusion. A regular security testing program/certification is required as part of secure value chain.

As MEC Infrastructures can span a wide geographical distribution and be located in challenging environments, maintaining a uniform data-center level of physical security is a significant challenge. A potential flaw in physical security of any MEC hardware may result in physical attack on the infrastructure. Physical security and environmental vulnerabilities of MEC hosts may arise due to improper physical and environmental security of edge computing facilities, improper security monitoring of edge computing facilities, etc. Control measures to ensure security of physically isolated areas include earthquake-proofing, automatic fire control equipment, monitoring by a remote office to detect facility failures, physically secure perimeters, supporting automatic alert function, etc. The physical security may not be fully guaranteed in an MEC environment and critical MEC components (e.g., security end points and crypto functions) need to be implemented in HMEEs (Hardware Mediated Execution Environments), e.g. Intel SGX or ARM TrustZone.

APIs are a well-known subject of multiple attack types, as they are exposed to external access. The common API Framework (CAPIF) is used by 3GPP as the standardized means to support providing and accessing APIs (and ETSI MEC is fully aligned with CAPIF). From a software development point of view, compliance with CAPIF should be ensured during API design and implementation phases. Further, the vulnerabilities in the service-based interface (SBI) of MEC components can include improper transport layer protection of data transferred over internal interfaces and improper verification of identity and access control to authorized MEC applications. In that perspective, SBI of network functions should provide adequate protection of access and data in transit. The confidentiality and data integrity of all messages should be ensured by using TLS on each interface. Appropriate security controls are required for protecting sensitive data storage, processing, and transfer by MEC applications. The MEC platform should authenticate all MEC application instances and only provide them with the information for which the application is authorized. OAuth 2.0 based on X.509 client certificates are used for authorization of access to RESTful MEC service APIs defined by ETSI ISG MEC. In case of service-producing applications defined by third parties, other mechanisms such as standalone use of JWT can be used to secure related APIs.

In addition, since MEC is based on virtualized infrastructure, it needs to include real-time Security Management based on NFV specifications [ref. SEC-013]. Especially when deploying MEC in NFV environments, MEC should be considered as part of a whole system real-time security monitoring and management strategy. Insufficient/improper monitoring mechanisms of MEC components can result from insufficient logging of security events for MEC App and MEC host. Appropriate mechanisms for collection and processing of security events should be in place, where the log functions should upload log files securely to a central location or to an external system. Secure transport protocols should be used. The security event log should be access controlled to allow only privileged users to have access to the log files. Critical event logs should be enhanced with mechanisms to audit them by independent third parties, preserving their *arrow of time* and their links to the identities of the involved elements. As part of regulatory issues, the European regulation (NIS-Directive) expects isolation of physical and logical components of critical services from services with low criticality. The MEC system need to support regulatory requirements for lawful interception and retained data based on ETSI and 3GPP standards (e.g., in ETSI TS 101 331, ETSI TS 102 656 and 3GPP TS 33.126).

2.2.1 Infrastructure security and physical protection

Ensuring physical protection of critical components and sensitive parts of the MEC network is crucial. For example, considering where the components are deployed and used, like a MEC used in hospitals or Railway stations. Access should be granted only to a limited number of security observers and qualified staff. Access by third-parties, contractors, and employees of suppliers/vendors, should be limited and monitored.

Edge Computing environments (in a local datacenter or micro-data center) might have many distributed clouds with nodes located in potentially poorly secured environments and likely running critical workloads, that bring a new set of physical security challenges. To prevent the hardware and software tampering of MEC, platform security, platform management security, data storage and transmission security should be enhanced. Insufficient encryption of sensitive data can lead to data breach, unauthorized disclosure & sharing of sensitive data and internal fraud. In absence of valid Certificates and lack of peer authentication, there is an increase in risk of Man in the Middle (MITM) attack. It could be needed to deploy a Certificate Lifecycle Management system with CA and HSM and ensure that cryptographic key material, shared secrets and passwords and similar security-critical data are not disclosed or tampered. Access to private keys should be strictly controlled and monitored. HSM to generate encryption keys and store home network Private key in HSM & perform crypto operations to be used. To authenticate peer MEC application exchanges communication inside the network, it should be ensured consistent encryption of sensitive data across CNFs/VNFs with granular access control using a centralized encryption key management across CNFs/VNFs from multiple vendors & HW storage providers.

2.2.2 Data protection

Lack of proper evaluation and implementation of advanced and adequate technology solutions (Data loss protection, DLP, Data Classification, CSPM, Container Security, etc.) related to Cloud Security increase the risk of an incident occurring in these critical environments. A cloud evaluation framework (including processes and guidelines) to compare and choose the cloud landing zone and corresponding cloud security solutions that fits the MEC ecosystem therefore should be created. Inadequate BCP/DR (Business Continuity Plan and Disaster Recovery) mechanisms for restoration of business services may not provide sufficient Edge security functionality resumption in the event of an outage. Here, Cyber Resiliency Capability will enable the MEC ecosystem with advanced capabilities to prepare, respond, and recover when a cyberattack happens.

2.2.3 User security and Data security

If, during MEC operations, security activities such as backup and restore, operational maintenance and equipment disposal are not performed consistently and effectively, the risk of data loss and system failure increases and potentially resulting in disruption of business operations. Thus, enhancement in the Backup management capability with a prominent data Security and Privacy program is required. The MEC platform should authenticate all MEC application instances and only provide them with the information for which the application is authorized. OAuth 2.0 based on X.509 client certificates are used for authorization of access to RESTful MEC service APIs defined by ETSI ISG MEC. In case of service-producing applications defined by third parties, other mechanisms such as standalone use of JWT can be used to secure related APIs [ref. 3GPP TR 33.839] and ETSI GS MEC 009 [ref. MEC-009] mandates support for RESTful API using HTTPS (HTTP over TLS (also known as HTTPS) using TLS version 1.2 or 1.3 (as defined by IETF RFC 5246 and RFC 8446). Implement Internet Protocol Security (IPSec) for securing IP communication and strong authentication mechanisms and using TLS with Edge Security Service to protect edge interfaces [ref. 3GPP TR 33.839].

2.2.4 Network Security Layer and Application Security Layer

Increasing entry points increases the number of attack surfaces in MEC such as in IoT use cases, raising challenges for Edge security. Weak IoT Security and poor certificate management may eventually increase the attack surface area. False or rogue MEC gateway can be protected by means of strong authentication mechanisms with the help of PKI infrastructure. There are many main attack surfaces related to MEC which we need to protect, firstly, inside surface that is mobile backhaul inheriting vulnerabilities, secondly, public facing internet attack, third party application or RESTful APIs and IoT devices which may cause DDOS or flooding attack (e.g., signaling) on Edge. For protection from these attack surfaces, building of Zero Trust principal is required. The traditional security principles do not consider enough insider and third-party threats when it comes to access management and infrastructure segmentation. The MEC network communications shall be secured for both internal and external networks. It will help to make the network more hardened and protected from any type of unauthorized east-west traffic or lateral moment inside the network. No users or account, resources, control plane, user plane and management plane signaling shall be trusted on the basis of their location or the location of the network or applications. It is proposed in [ref. 3GPP TR 33.839 and TS 23.558].

2.3 Security aspects for MEC federation

MEC federation is a topic of active discussion, with related requirements and specifications being developed, also starting from the requirements defined by GSMA OPG (Operator Platform Group), and in collaboration with 3GPP. This new concept of MEC Federation is also captured in a recent publication of GS MEC 003, where a new variant of the MEC Architecture is foreseeing the inter-MEC system communication in that perspective. Having this kind of heterogeneous scenario, with related exchange of information, and also edge resource sharing among operators (in collaboration with edge computing service providers and partners), implies a number of security threats. These have been analyzed by GSMA in their recent publication [ref. GSMA-PRD], by providing a categorization of threats, in order to facilitate the normative work from SDOs. Here are the main categories of security threats for the MEC Federation:

- Access Threat vectors
    - These are at locations that connect a UE to the OP system.
    - In ETSI ISG MEC, the vulnerabilities are on the RAN link from the UE to the BTS/eNB/gNB, between the UE application and the UE client and in the UE itself
- Architecture Threat vectors
    - vulnerabilities that occur in the overall architecture of a system or its components.
    - Therefore, those vulnerabilities may manifest themselves in OP functions as well as in reference points.
    - The significant categories of threat vectors have to do with validating containers and VMs, both in a particular platform and upon migration to other platforms and with performing traffic steering to applications in a secure manner.
- Core Threat Vectors
    - They affect the core 5G network, orchestrators, resource managers, controllers, and applications.
    - In OP's case, where implementations of these components map onto Capabilities Exposure and Service Resource manager roles, all of the Core threat vector types appear to be relevant.
- Edge Threat Vectors
    - cover platform managers, VIMs, MEC platform connectivity and connectivity of MEC apps operated at non-local base stations.
    - These threat vectors appear to map to the EWBI.
- Other Threat Vectors
    - areas that do not fit at a specific reference point and which manifest because of functionality, not architecture
    - For example, charging/billing
- Privacy Threat Vectors
    - Data privacy, location privacy, identify privacy

- Computational Offloading privacy threats
- Etc.

In order to satisfy the OPG requirements, the standardization work in ETSI MEC (but also in 3GPP) is expected to consider this GSMA work and put necessary measures in place to enable the actual deployment of the MEC Federation, which is very critical for operators and service providers.

3 Security standards for MEC technology

MEC security relies on specifications provided by other recognized bodies to address specific aspects, especially ETSI ISG NFV for infrastructure virtualization and management, the Trusted Computing Group (TCG) for physical platform security, and IETF specifications for securing access to MEC services.

Furthermore, 3GPP TR 33.848 [ref. TR33.848] is investigating the security consequences of virtualization of 3GPP NFs. This 3GPP report is applicable to many MEC use cases where the need for additional security controls is higher than in core network data center implemented network functions. It is expected to result in additional ETSI NFV security requirements that can be utilized for MEC.

Finally, Security Assurance is an important topic which starts to be required by regulations for 5G infrastructure components such as MEC. While the traditional Common Criteria technology (as in ISO 15408 [ref. ISO-15408}) remains a global reference for Security Assessment, tailored schemes that address the specific constraints of 5G ecosystems, such as GSMA NESAS, are expected to play an important role in this respect.

3.1 ETSI ISG NFV support for security

Multi-access Edge Computing (MEC) and Network Functions Virtualization (NFV) are complementary concepts. One of the main MEC components at host level is the virtualization infrastructure, which provides compute, storage, and network resources for the MEC Applications in the same way with NFVI defined in ETSI ISG NFV. The NFV Security WG (NFV SEC) has concentrated on analyzing threats to security in virtualized environments and published series of specs and reports on security requirements and solutions for NFVI in the past few years.

The MEC architecture has been designed in such a way that a number of different deployment options of MEC systems are possible. In this perspective, the GS MEC 003 specification introduces an architectural variant for MEC in NFV. This variant (depicted in the figure 4 below) allows to instantiate MEC applications and NFV virtualized network functions (VNFs) on the same Virtualization infrastructure, and to re-use ETSI NFV MANO components to fulfil a part of the MEC management and orchestration tasks.

As a consequence, especially when talking about this “MEC in NFV” deployment option, all the solutions designed to address NFV security should be potentially reused in MEC systems, when applicable (e.g., to MEC Platforms and MEC applications, which are deployed as VNFs).

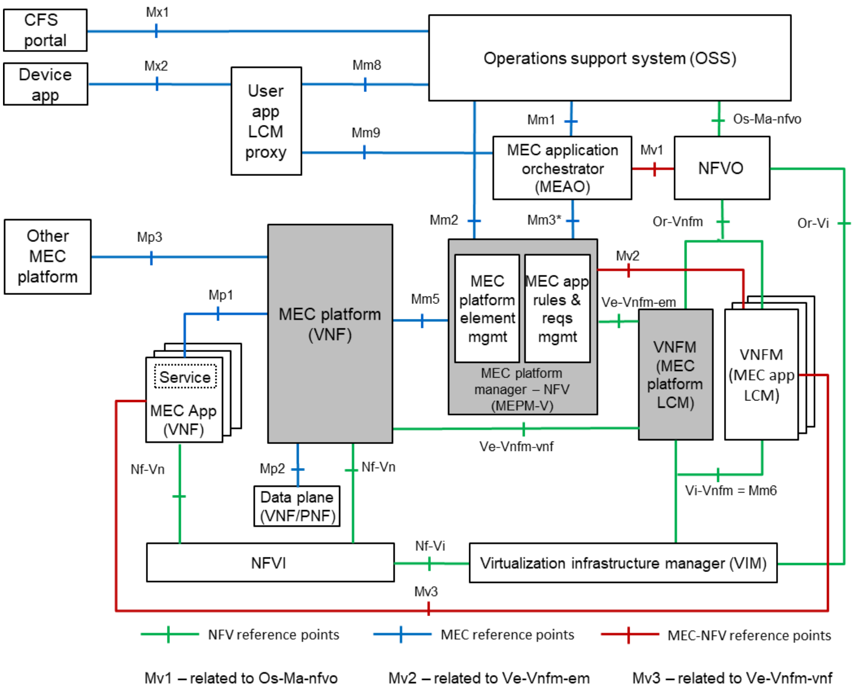

Figure 4: Reference architecture variant for MEC in NFV ([ref. MEC-003])

The potential security problem of NFVI is generally stated in ETSI GS NFV-SEC 001 (ref. [SEC-001]), which includes secured multi-layer administration, secure crash, performance isolation, authenticated time service, etc. To addresses multi-layer administration, use cases and technical approaches, ETSI GR NFV-SEC 009 (ref. [SEC-009]) seeks to provide methods, capabilities, procedures, and assurances of various strengths based on requirements and available technologies and techniques - that safeguard Virtual Machines or Containers running on a virtualization host.

ETSI GS NFV-SEC 012 (ref. [SEC-012]) takes this further by defining additional security requirements for sensitive functions (or components within larger functions), such as use of Hardware Mediated Execution Environments (HMEEs). Sensitive components include cryptographic tunnel end points, security functions and Lawful Interception functions. A list of technologies and measures from various domains is provided to meet the requirements of the various use cases, including memory inspection, secure logging, OS-level access control, secure storage, etc.

To facilitate the secure and automated NFV deployment, security monitoring and management use cases and security requirements are investigated in ETSI GS NFV-SOL 013 (ref. [SOl-013]). This is being further extended in ETSI GS NFV-SEC 024 to provide a "whole system" security monitoring and management framework. Potential methodologies and placement of security visibility and control elements are proposed to fulfill the identified requirements, e.g. NFV Security Agents deployed in NFVI domain to report the telemetry data from NFVI, Infrastructure Security Manager dedicated to security management in NFVI layer which builds and manages the security in NFVI.

NFV specifications also take a deep dive into the security and protocols necessary to securely support lawful interception in virtualization environment which include LI architecture (ref. [SEC-011]) and retained data protection (ref. [SEC-010]). The overall identified issues have dependency on the security of underlying virtualization infrastructure, e.g., physical control and alarms, post-incident analysis, secure key management, etc.

Security for NFVI and NFV MANO API is provided by ETSI GS NFV-SOL013 [ref. SOL-013] and ETSI GS NFV-SEC022 (ref. [SEC-022]). API security at the NFVI, MEC and MEC application layer (e.g., 3GPP NFs) needs to be carefully considered to ensure the APIs do not allow an attacker a single point of entry into all layers of the MEC environments.

NFV security WG are also exploring further features in the current release to make the NFVI secure enough for wide range deployment scenarios and use cases. The related specifications include container security defined in Draft ETSI GS NFV-SEC 023 [ref. SEC-023], isolation and trust domain defined in Draft ETSI GS NFV-SEC 026 [ref. SEC-026] and NFVI security assurance defined in Draft ETSI GR NFV-SEC 027 [ref. SEC-027].

In summary, on building the security of MEC architectural components, the security practices and specifications of NFVI produced in ETSI ISG NFV provide critical building blocks as part of a whole MEC system security design.

3.2 Security in ETSI ISG MEC Specifications

The major security emphasis in MEC specifications is on securing access to MEC service APIs by service consuming applications. ETSI ISG MEC standardizes a variety of MEC services by specifying implementation agnostic, RESTful APIs using HTTP. The ETSI GS MEC 009 specification [ref. MEC 009] defines design principles for RESTful MEC service APIs, provides guidelines and templates for the documentation of these, and defines patterns of how MEC service APIs use RESTful principles. The specification mandates support for HTTP over TLS (also known as HTTPS) using TLS version 1.2 (as defined by IETF RFC 5246). TLS version 1.3, defined by IETF RFC 8446, should be also supported. The specifications explicitly prohibit the use of HTTP without TLS or TLS versions preceding version 1.2.

The general principles defined in GS MEC 009 [ref. MEC 009] apply for all the APIs using Mp1 reference point between MEC Applications and MEC platform (thus applicable also to service producing MEC Applications exposing their services via the MEC platform). The ETSI GS MEC 011 specification [ref. MEC011] focuses on the functionalities enabled via the Mp1 reference point between MEC applications and MEC platform and also follows the above design principles defined by GS MEC 009, to allow applications to securely interact with the MEC system.

The MEC platform should authenticate all MEC application instances and only provide them with the information for which the application is authorized. MEC specifications mandate the use of the OAuth 2.0 for authorization of access to RESTful MEC service APIs defined by ETSI ISG MEC. The implementation of the OAuth 2.0 authorization protocol uses the client credentials grant type according to IETF RFC 6749 and with bearer tokens according to IETF RFC 6750. The framework assumes an AA (authentication and authorization) entity to which a MEC platform operator configures credentials and access rights. Clients first authenticate themselves with the AA entity using their credentials to obtain an access token. Clients then present this access token as the bearer token in all requests for MEC services to authenticate themselves. To mitigate DDoS attacks and other privacy concerns, the specifications recommend setting appropriate authorization policies which are then bound to access tokens. Policies may be set to restrict access to sensitive resources or to rate-limit requests from clients at service endpoints. Access tokens have a validity period after which they expire. They may also be revoked prior to expiry via the AA entity. Further, the specifications recommend anonymizations of real identities in MEC deployments.

OAuth 2.0 has the optional provision for scopes which may be defined at the level of resources, combinations of resources and methods, or combinations of resources and methods with specific values for parameters, or values of attributes in the payload body. For subscriptions, the subscription type can be used to scope the authorization and is expressed as a string named the permission identifier. Definitions of permission identifiers thus accompany MEC service specifications. The available authorization scopes for a service are made known to clients during service discovery. In place of OAuth 2.0 standard bearer tokens, AA entities in MEC deployments may also hand out JSON Web Tokens (JWT) (IETF RFC 7519). JWT have a compact representation and an extensible structure to directly encode application defined claims and entitlements into the access token. These may include OAuth scopes or roles to restrict access to MEC services. JWTs may be signed by the AA entity to become tamper proof and encrypted to not leak any application metadata. Thus, JWTs are self-contained and self-verifiable access tokens. A practical benefit of using JWT bearer access tokens is they allow fully decentralized and stateless enforcement of API security, not needing to continually query the AA entity upon requests to MEC services, thereby yielding a performance gain.

The only fully specified transport by ETSI for MEC service APIs is HTTP-REST. Alternative transports may also be used in applications that require lower latency or higher throughput than REST-based interactions can provide. Two examples are Publish-Subscribe (PubSub) protocols that rely on topic-based message brokers (e.g., MQTT), and Remote Procedure Call (RPC) frameworks such as gRPC. These transports may also employ different data serializations (e.g., Protobuf) instead of JSON. Support for new transports may be facilitated by the MEC platform, or alternatively exposed directly by MEC applications offering a service.

In this perspective, it is critical to support the encryption of data between MEC applications regardless of the chosen transport along with the means to restrict access to services. The TLS protocol is designed to handle encryption, authentication, and data integrity, and most transports (including HTTP-REST) rely on TLS to secure the communications channel. TLS credentials (e.g., X.509 certificates) are used to authenticate the endpoints and can further help identify peers in a TLS session by reading its identity from its certificate presented during the TLS handshake. A client identifier thus obtained can be used by MEC services to authorize requests from the client based on configured access policies and permissions. This is the primary approach with PubSub transports that do not support OAuth 2.0 authorization. Hence, the client identity forms the basis for enforcing authorizations within the transport-specific (e.g. MQTT) authorization model. Authorization scopes for such topic-based transports may also be specified by permission identifiers that map to topic names. RPC transports, on the other hand, like HTTP-REST support OAuth 2.0 authorization and scopes, and the service endpoints are responsible for enforcing the authorizations.

Lawful Interception (LI) and Retained Data (RD) play a crucial role in helping Law Enforcement Agencies (LEAs) to combat criminal activity. LI enables a LEA to perform electronic surveillance of chosen targets as authorized by the judicial process. In current mobile core networks, LI and RD solutions are inherent and supported by the available 3GPP standards. However, when implementing MEC, any traffic that originates inside a MEC system or arrives from a local breakout connection does not pass through the core network and could circumvent LI on the network. In this scenario, if the underlying network utilizes the CUPS (Control and User Plane Separation) architecture, then LI support still applies based on the 3GPP standards. For e.g., in a 5G network LI and RD solutions placed in the UPF (User Plane Function) could extend over to cover all MEC traffic. In MEC deployments where the core network does not support CUPS, some alternative solution may be needed, e.g., the introduction of a new entity e.g., LI Gateway (LIG), along with the provision to identify and store information on LI targets. With this in place, all traffic associated with LI targets needs to be duplicated and directed towards the LIG to satisfy the regulatory requirements as they pertain to LI and RD. By the way, these solutions are only needed for networks not supporting CUPS (i.e., in LTE systems before Rel.14), as for newer systems (i.e. for LTE Rel.14 on, and especially for 5G Core, which is "CUPS-native") 3GPP LI&RD is natively supported for MEC application traffic as it is for any application traffic passing the UPF.

3.2.1 Additional considerations for end-to-end MEC security

As said, MEC environments are heterogenous, i.e. composed by the interaction of different players, each of them with different roles and duties, where the various elements of the system can be deployed managed and operated by different stakeholders. Figure 5 below, elaborated from 3GPP TS 28.814, shows the roles and relationship of the various actors involved in the deployment of edge computing services (see also annex B in TS 23.558).

In particular, we have:

- The application service provider (ASP), responsible for the creation of EAS / MEC applications, and Application Clients (AC), representing the edge computing application running in the server and UE client, respectively.
- The edge computing service provider (ECSP), responsible for the deployment of edge data networks (EDN) that contain EAS / MEC applications and EES /MEC platforms.
- The PLMN operator: responsible for the deployment of 5G network functions, such as 5GC and 5G NR.
- The UE, where Application Clients (AC) and EECs are running. Furthermore, also other kinds of end-devices can host some application elements (e.g., especially in IoT environments).

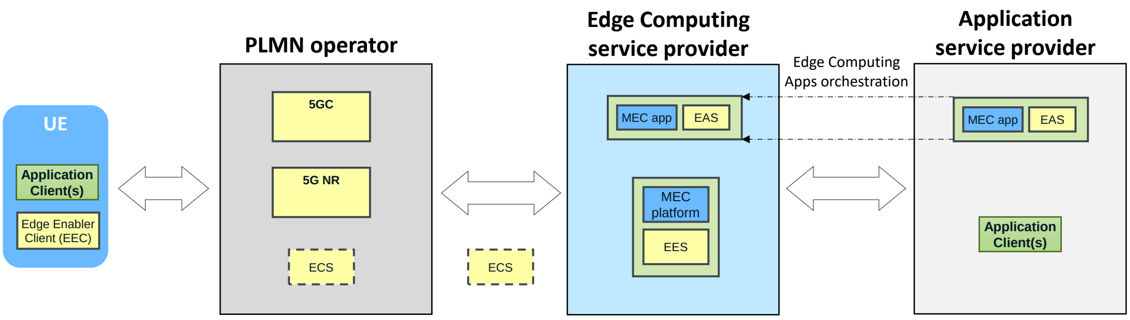

Figure 5: Relationship of service providers in the edge computing network deployments

In this heterogeneous scenario, talking about end-to-end MEC security implies to consider the impact on the elements coming from all stakeholders involved in the system. In that perspective, MEC should pay attention to the vulnerability and integrity of any third-party elements.

In particular, when it comes to MEC platforms and third-party software components, a large number of third-party mirrors come from the open-source community, and there is usually the possibility of vulnerability and tampering. MEC platform is the running environment of third-party mirroring. It must be capable of identifying the vulnerability and integrity of mirroring. The MEC platform should formulate different baselines for specific application scenarios. The baselines can refer to CIS (Center for Internet Security) or can be extended. The MEC platform should also be able to check the integrity of the third-party image to prevent attackers from inserting malicious code into the image. MEC applications should provide their own security parameters for MEP/MEPM to monitor and display. For example, CPU/memory occupation and service port opening are very important for the normal operation of MEC-app.

3.3 ETSI TC CYBER support

The economic potential of IoT largely addresses the long tail of the demand spectrum, i.e. use cases that may differ substantially to each other, both within and across the industry segments they address. In addition, sectorial requirements, and regional regulations in regard to privacy and security can further complicate the whole picture not only in terms of overall performance but also compliance.

In that regard, end-to-end security in MEC systems is of upmost importance, considering that the MEC platform can handle application traffic and that the various application elements may reside not only in MEC Hosts but also on UEs and end-devices, where the security capabilities of the latter come into the end-to-end picture of security.

As a baseline of requirements for the IoT, TC CYBER has published consumer IoT requirements for security and data protection primarily in the EN 303 645 and TS 103 701 standards [ref. EN30364] and ref [TS103701]. The first document specifies security and data protection provisions for consumer IoT devices that connect to network infrastructures and interact with associated services:

Table 1: Baseline security requirements for consumer IoT.

• No universal default passwords	• Implement a means to manage reports of vulnerabilities
• Keep software updated	• Securely store sensitive security parameters
• Communicate securely	• Minimize exposed attack surfaces
• Ensure software integrity	• Ensure that personal data is secure
• Make systems resilient to outages	• Examine system telemetry data
• Make it easy for users to delete user data	• Make installation and maintenance of devices easy
• Validate input data	

Overall, EN 303 645 specifies 68 provisions, 33 of them being mandatory and 35 recommendations. All are addressed by TS 103 701, which defines a conformance assessment methodology in companion to EN 303 645. Particularly in regard to vulnerabilities, TR 103 838 provides guidance on vulnerability disclosure policy, action plans and generic advice on how to respond to and handle vulnerability disclosure.

The deployment of IoT devices in a MEC environment can involve additional support that an IoT device may require, e.g., due to security constraints, power limitations, and compute or communication capabilities [ref. MEC-033]. As identity management is a pillar of any robust security architecture,

TC CYBER is developing a secure and manageable identity management scheme applicable to IoT devices in a MEC environment [ref. TS103486]. The scheme addresses the requirements of cryptographic methods that establish trust in Authority-Attribute trees. The latter provide data structures that represent identity information, which can be encoded in a suitable ontology (e.g., SAREF [https://saref.etsi.org/].

In addition, ETSI TS 103 742 covers basic good practices for the cybersecurity of communication network such as one that the deployment of IoT applications in a MEC environment may involve [ref. TS103742]. These address policy aspects and the lifecycle thereof:

Table 2: Good practices for the cybersecurity of communication networks

• Organize for security	• Securely store credentials and security-sensitive data
• Communicate securely	• Ensure that personal data is protected
• Signaling integrity and protection	• Software and Virtual functions
• Back up and contingency planning	• Outsourcing of infrastructure and services
• SIM security and tokens	• Physical security of assets
• Supply chain security	• Vulnerability Disclosure
• Testing and auditing	• Accountability and monitoring of actions
• Fraud detection and billing integrity	• Legal conformance
• Training and awareness	

3.4 TCG (Trusted Computing Group)

Trusted Computing is a set of techniques dedicated to making sure that anything which is being executed on a computer actually does what it should be doing. This is a very loaded statement, which must be clarified. Clearly, no general-purpose computer can know either what a particular program should not be doing or whether it's doing what it should be doing. Let's make this specific then, Trusted Computing is a set of techniques which allows a computer to restrict or grant privileges to a program (e.g., privilege to run, privilege to access data, etc.) only if a well-defined measurement of the state of such program, data, etc. corresponds to a secure reference.

As noted in our discussion of use cases, platform security is a particularly acute issue for MEC given the security challenges associated with the highly distributed nature of MEC clouds. As such, the use of Trusted Computing concepts in MEC deployments is strongly encouraged.

In practice, platform trust is achieved through reliance on a small, specialized processing element – a Trusted Platform Module (TPM), designed to fulfill a number of roles in a secured computing platform. Some of the key roles are as follows:

- An immutable root of trust. A TPM represents a commonly trusted and immutable (because fully HW based) initial processing step, to which trust in other processing steps can be bootstrapped.
- A TPM polices access to secure memory, which can be used to store certificates that are then used to attest to security of system components. This "secure memory" is immutable, except via TPM (usually implemented as part of the TPM itself).

Note that the concept of a TPM only works if it is commonly trusted - i.e. everyone (or almost everyone) agrees that a TPM represents a sufficiently secure root of trust. This requires the definition of the TPM to be open, mutually agreed on, and well-tested - i.e. standardized.

The Trusted Computing Group (TCG) (https://trustedcomputinggroup.org/) is the organization that defines widely accepted TPM standard as well as a number of related standards. The importance of TCG in the computing ecosystem is highlighted by the acceptance of the latest baseline TPM specification [ref. TCG1] as an international ISO/IEC standard ISO/IEC 11889:2015.

3.5 Other relevant standards

3.5.1 3GPP SA3

Even if MEC (as per the acronym) is access-agnostic, 5G deployments are a targeted key environment, and then 3GPP standardization is relevant when it comes to 5G support for edge computing. This subclause presents an overview of security aspects from 3GPP [TR33.558][TR33.839] to summarize the security enhancements on the support for Edge Computing in the 5G Core network defined by SA2 [ref. TR23.748][ref. TS23.548], and application architecture for enabling Edge Applications defined by SA6 [ref. TS23.558] and [ref. TR 23.758] (referred as EDGEAPP architecture, including entities such as Application Client (AC), Edge Application Server (EAS), Edge Configuration Server (ECS), Edge Enabler Client (EEC), Edge Enabler Server (EES), as shown in Figure 6 below). The EDGEAPP architecture defined by TS 23.558 introduces new interfaces such as EDGE-x (i.e., EDGE-1,4,5 are type A interfaces between UE and Edge servers; EDGE-2,7,8 are type B interfaces between 3GPP core and Edge servers; and EDGE-3,6 and 9 are type C interfaces between Edge servers).

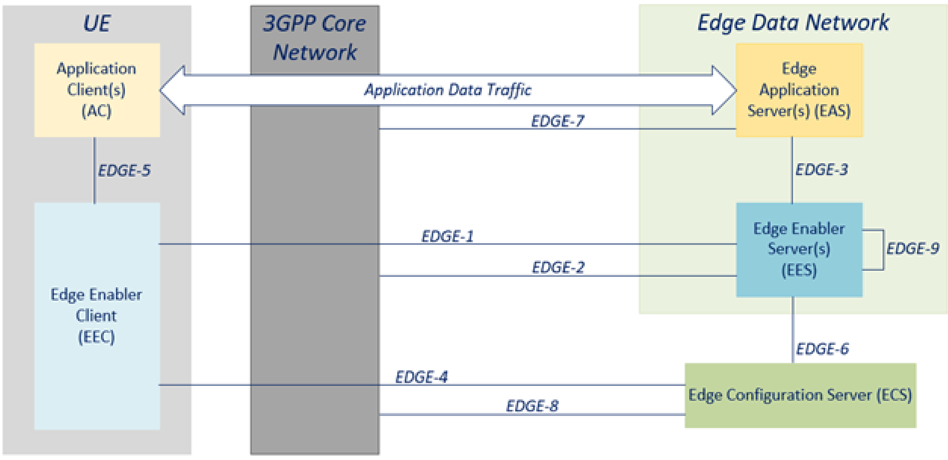

Figure 6: Architecture for enabling edge applications [TS23.558]

A key aspect for edge computing is the support of EAS discovery and Edge relocation in various connectivity models, and the network information provisioning to local applications with low latency (as described in TS 23.548). in that perspective, the TR 33.839 contains indeed a security key issue on this EAS discovery procedure, aiming to protect the EAS discovery message, securely expose the network information to the local applications, and to authorize the UE EAS service access during Edge Data Network relocation with seamless change. In particular, the key issue describes the usage of an enhanced DNS forwarder called as 'LDNSR', that supports EAS discovery using DNS based on the UE 5GC connectivity information. The Session Management Function (SMF) provides the information on UE 5GC connectivity to the LDNSR, where the messages between the SMF and the LDNSR is confidentiality, integrity and replay protected (i.e., to prevent attackers to eavesdrop or manipulate DNS message to redirect to a compromised Edge server) using existing SBI based security aspects specified in TS 33.501 [ref. TS33.501].

Regarding the normative work published by SA3, it is important to mention the TS 33.558. According to this specification, edge services discovery is secured by reusing the DNS security aspects (i.e., DNS over (D)TLS, where a TLS cipher suite that supports integrity protection need to be negotiated) as described in TS 33.501.

The TS33.558 normative work related to support for enabling edge application also includes the following security aspects:

i. mutual authentication and authorization between EEC and ECS over EDGE-4 interface (e.g., Authentication method may be based on TLS certificates, usage of AKMA or GBA to establish PSK for TLS. The ECS can be configured with information on authorization methods (i.e., token-based or local authorization) used by EESs),

ii. mutual authentication and authorization between EEC and EES over EDGE-1 interface (e.g., Authentication method may be based on TLS certificates, usage of AKMA or GBA to establish PSK for TLS. For authorization of EEC by EES, if provided by ECS, the EEC can use OAuth 2.0 access token. Otherwise EES can authorize the EEC based on local authorization policy),

iii. mutual authentication and authorization between EES and ECS over EDGE-6 interface (i.e., TLS based mutual authentication and authorization based on local authorization policy),

iv. mutual authentication and authorization between EAS and EES for EES capability exposure to EAS over EDGE-3 interface (i.e., EES may expose the network capabilities of 3GPP core network to the EASs based on CAPIF architecture specified in TS 23.222, where CAPIF security specified in TS 33.122 [ref. TS33.127] is used for authentication and authorization. If CAPIF is not used, TLS based mutual authentication and local authorization policy can be used).

The interface security for EDGE-1-4 and EDGE 6-9 includes confidentiality, integrity and replay protection (i.e., to prevent any attacker from eavesdropping, manipulation and/or replay). Further for the interfaces EDGE-1/4, the EEC, EES and ECS supports TLS and HTTPS as in RFC 7540 and RFC 2818, where TLS is used for transport protection. For interfaces related to EDGE-2/7/8, if NEF APIs are used, then protection of NEF and AF interface and CAPIF is supported as defined in TS 33.501. Alternatively, if SCEF APIs are used, then security procedures for SCEF-SCS/AS reference points (i.e., use of TLS) defined in TS 33.187 can be reused. Finally, for the interfaces EDGE-3/6/9, the EAS, EES and ECS supports TLS and HTTPS, where TLS is used for transport protection unless security is provided by other means such as physical security.

Additionally, 3GPP SA3 has concluded the TR 33.839, that captures the agreed protection mechanisms in TS 33.558 which includes interface protection, service authorization and user consent [ref. TS33.558]. Furthermore, a phase2 study [TR33.739] has been launched in March 2022 to study additional issues in MEC. The main target is to support roaming in various scenarios, e.g., local traffic routing, authentication between entities located in different PLMN, etc. In addition, 3GPP SA3 is working on two Technical Reports on Security Impacts of Virtualization [TR33.848] and Security Assurance Methodology (SECAM) [ref. TR33.818], leading to the introduction of a set of Security Assurance Specifications (SCAS) for 3GPP virtualized network products. Both of these reports explore the additional threats and mitigations required to design, test, and deploy functions in a virtual environment. MEC use cases represent many of the higher risk threat scenarios identified by SA3. In particular, TR 33.848 has currently identified 28 security key issues which are also applicable to MEC: while a number can already be addressed through existing standards and best practice security approaches discussed in this white paper, other require development of new security solutions or deployment mitigations.

On the other side, TR 33.818 provides security assurance mechanisms in 3GPP virtualized environment: the document already considers threats related to the integration of ETSI VNF concepts and interfaces within the 3GPP virtualized system, including limited security of the interface between 3GPP VNF and VNFM, the interface between virtualization layer and hardware, and the interface between virtualization layer and the VIM. Different generic virtualized network products (GVNPs) are defined in the document, including type 1 (implementing 3GPP defined functionalities only), type 2 (implementing 3GPP defined functionalities and virtualization layer), and type 3 (implementing 3GPP defined functionalities, virtualization layer, and hardware layer). Compared to physical network product, GVNP has also two types of logical interfaces, i.e. execution environment interfaces and remote logical interfaces. The remote logical interfaces are interfaces which can be used to communicate with the GVNP from another network node and also include the remote access interfaces to the GVNP for its maintenance through e.g. an Element Management (EM), a Virtualized Network Function Manager (VNFM).

The 3GPP threat analysis is based on the ETSI NFV reference architecture, described in the following figure:

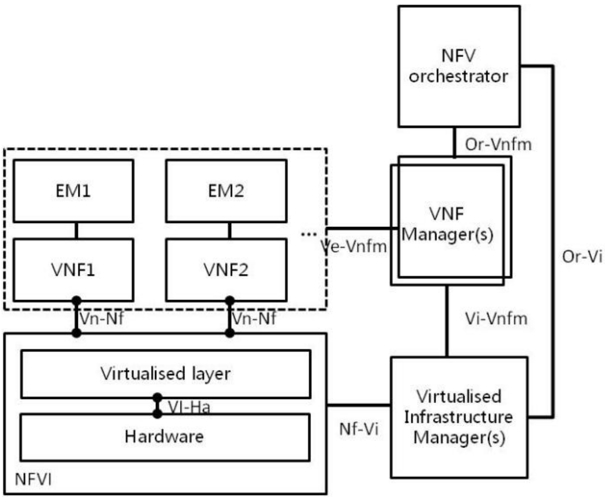

Figure 7: ETSI NFV reference architecture (ref. [ETSI-2014])

For the GVNP model of type 1, the external interface to the ETSI model is represented by Vn-Nf, while for the GVNP model of type 2, the Vn-Nf between VNF and the virtualised layer is an internal interface. Type 2 GVNP, in addition to the interface between the VNF and VNFM (ref. Ve-Vnfm), has the following ETSI NFV specified interfaces: Nf-Vi (between virtualization layer and VIM) and VI-Ha (execution environment interface). For the GVNP model of type 3, both interfaces (i.e., Vn-Nf and VI-Ha) are internal interfaces; therefore, only ETSI NFV interfaces are Ve-Vnfm and Nf-Vi.

SA3's sub-group SA3-LI are also discussing security requirements to support Lawful Interception in an MEC environment and work is on-going as part of wider virtualization LI security requirements [ref. TS33.127].

In the context of 3GPP security, it is worth mentioning the Network Equipment Security Assurance Scheme (NESAS) as well, jointly defined by 3GPP and GSMA, provides an industry-wide security assurance framework to facilitate improvements in security levels across the mobile industry [NESAS-2.0]. NESAS defines security requirements and an assessment framework for secure product development and product lifecycle processes, as well as using 3GPP defined security test cases for the security evaluation of network equipment. NESAS provides a security baseline to evidence that network equipment satisfies a list of security requirements and has been developed in accordance with vendor development and product lifecycle processes that provide security assurance. NESAS is intended to be used alongside other mechanisms to ensure a network is secure, in particular an appropriate set of security policies covering the whole lifecycle of a network. The scheme should be used globally as a common baseline, on top of which individual operators or national IT security agencies may want to put additional security requirements.

3.5.2 ISO/IEC 15408

While 3GPP SCAS and GSMA NESAS are targeting security of products from a 5G perspective, MEC systems are also more in general including IT products. In this perspective, MEC infrastructure owners should also pay attention to established procedures for security verification, evaluation, and certification as the one defined by ISO/IEC 15408, also known as Common Criteria for Information Technology Security Evaluation (ref. [ISO-15408]). This standard is meant to be used as the basis for evaluation of security properties of IT products and establishes the general concepts and principles of IT security evaluation by also specifying the general models for this evaluation. In other words, ISO/IEC 15408 defines a framework for *specifying* the *functional* and *security* requirements of a computer system operating in a given *environment* and subject to certain *assurance* levels. On the one hand, this framework allows vendors to *implement* a computer system, e.g., the MEC Platform, according to common specifications and, on the other hand, testing laboratories to *evaluate* products and to determine the delivered *assurance* level. In particular, ISO/IEC 15408 specifies seven Evaluation Assurance Levels (EAL) describing the rigorousness and the extensiveness of an evaluation: with EAL 1 being the most basic and EAL 7 being the strictest. It is worth noticing that higher EALs do not necessarily imply better security, it only means that the security assurance has been more extensively verified. As of today, computer systems operating in critical and safety-sensitive environments (e.g., automotive, industrial, robotics, etc.) are often requested to meet a high EAL. Consequently, a MEC system (or a component of it) operating in those kinds of environment is equally expected to be evaluated according to these same common criteria, including recent criteria related to information security, cybersecurity, and privacy protection (ref. [ISO-15408-2]).

3.5.3 NIST and ATIS

The National Institute of Standards and Technology (NIST) published a new report for hardware-based security techniques and technologies to reinforce server platform security and data protection for cloud data centers and edge computing. The report is looking at mixed cloud data center and edge computing environment where attack surfaces have increased. NIST recommends the physical platform should be the first layer of defense on the edge and cloud, and outlines solutions to minimize security threats and argues that the firmware or software vulnerabilities can be addressed with hardware-enabled security techniques. To increase platform integrity, the NIST recommends hardware security modules such as trusted platform module (TPM) to generate cryptographic keys and protect sensitive information.

In addition to the hardware-based solutions and driven by White House Executive Order 14028 to improve the nation's security, NIST and NTIA have been working on defining mechanisms to secure the supply chains[1] primarily addressing the need for Software Bill of Materials (SBOM) and securing the software development lifecycle. Moreover, the Alliance for Telecommunications Industry Solutions (ATIS) has developed a 5G Network Assured supply Chain specification[2] defining three levels of assurance.

[1] https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1

[2] https://access.atis.org/apps/group_public/download.php/66150/ATIS-I-0000090.pdf

3.5.4 SASE and MEF

The term Secure Access Service Edge (SASE) was brought up by Gartner in 2019 [ref. SASE2019] to define a category of hardware and services used to enable edge security. They describe SASE as a way that successfully combines WAN capabilities with extensive network security functions that support secure access. Today, providing managed security functions in the cloud is a reality thanks to SASE that integrates managed security in the cloud with think SD-WAN on customer premises. Security functions that can be offloaded from corporate network premises to the cloud. SASE is ideal for an edge provider that has SD-WAN offering for its corporate customers. The MEC location on the edge provides an opportunity for the telcos to bring their SASE further towards the network edge and provide a low latency SASE offering. In fact, s one of the key principles of the Gartner's SASE model is that instead of forcing (via "tromboning") various entities' traffic to inspection engines entombed in boxes in the data center, it is needed to invert the thinking to bring the inspection engines and algorithms closest to where the entities are located. Therefore, MEC can be a great opportunity to effectively bring SASE service capabilities. In this perspective, MEF (Metro Ethernet Forum), as a global industry association of network, cloud, and technology providers, is working on standardizing SASE offering for such managed service providers[3].

4 Security regulations

In the context of MEC security, it is also worth to briefly illustrate cybersecurity regulation potentially applicable to edge computing and in particular the ENISA EUCS scheme and the NIS directive. Relevant requirements coming from regulation must be fed into the design and operation processes.

The candidate EUCS scheme (European Cybersecurity Certification Scheme for Cloud Services) [ref. EUCS2020], prepared by the ENISA Ad Hoc Working Group (AHWG) defines a candidate EU cybersecurity certification scheme on cloud services. The EUCS is part of the European cybersecurity certification framework since it follows the European Commission's request under Article 48.2 of the Cybersecurity Act (ref. EUCSA). The requirements defined in the scheme draws from many different sources (the German C5 scheme, the French SecNumCloud scheme, and from the proposals in the CSP-CERT report, as well as from principles in other schemes used in Europe). The EUCS scheme addresses the certification of the cybersecurity of cloud services. The EUCS scheme is intended to be a horizontal scheme, applying the same criteria to all cloud services; therefore, it also includes the Edge Cloud. Both the design and implementation of the cloud service are involved. As such, defined criteria apply to the security features and the whole edge Lifecycle's essential processes (development, deployment, and operation).

The Directive on security of network and information systems (the NIS Directive) is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU. The goal of the NIS directive [EU-NIS] is to protect critical infrastructure that ensures national security[4]. The Commission has subsequently submitted a proposal, known as the NIS 2.0 Directive to replace

[3] https://www.mef.net/service-standards/overlay-services/sase/

[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive); Link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

the original NIS Directive [5]. The new directive strengthens the risk and incident management and cooperation and widens of the scope of the rules. It also includes aspects that were left uncovered, such as the security of supply chains, and aligned the text with sector-specific legislation[6]. When a critical service needs to be deployed in the Edge, as is the case of some MEC use cases, the Edge Cloud becomes part of the critical infrastructure. In this case, the critical service deployment should reference the NIS directive and be operated in an area with a security level compatible with this criticality. This constraint imposes strict requirements on the level of isolation around the service and the resources it accesses. Improper isolation of resources has an important impact on the reliability of the critical service. For this reason, sharing of physical and logical resources with components that have not the same criticality should not be allowed. This aspect involves various MEC components such as the virtualization infrastructure, MEC host, MEC Platform.

5 Future evolutions of security support

The foreseeable evolution of edge computing is obviously aligned with those of the related infrastructural technologies, cloud, and networking. Consequently, the security challenges will be associated with those in these technologies, with the additional “edge twist” of being an extremely distributed cloud very much relying on network functionality.

Trends such as a more radical approach to cloud-native like the *serverless* proposals, the consolidation of hybrid clouds and NFV through the seamless integration of computing and networking into the so-called *in-network computing*, the integration of acceleration mechanisms both in computing and network forwarding, the pervasiveness of AI and its strong dependency on dependable data flows, and for sure the evolution of networks towards the *6G* goal, will have to be considered in any forecast of the coming security challenges for edge computing technologies.

Along these main trends, there are several base security enablers that will require future standardization to support the evolution of edge computing. In the following we briefly analyze the hottest topics with respect to their standardization requirements.

Confidential computing is intended to protect data while being processed and stored, by means of hardware-based isolation for the processing of payloads. It is currently based on vendor specific designs and threat models, as well as requiring a standardized approach to hardware-based acceleration.

Network topology attestation implies the ability to verify that a given network flow, at any given plane, is going to pass through the specific functions, optionally preserving a given order. To this purpose, inline operation and management and programmable packet forwarding devices, open a promising way for completing attestation mechanisms.

AI pervasiveness poses some challenges in terms of privacy, especially when highly centralized data stores are in use. In order to address these privacy challenges and make use of distributed data, new techniques enable collaborative AI/ML without centralized data. As such, accurate AI/ML models that reflect a wider

[5] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS2 Directive); Link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN.

[6] The text reached its final stage and, at the moment of the publication of the present white paper, the Council and the European Parliament have reached a provisional agreement.

dataset can be trained, while retaining the privacy and locality of private and sensitive data. The applicability of edge computing is evident, with a clear need for common, secure and standardized data and knowledge representation models.

The advent of disintermediation mechanisms provided by Distributed Ledger Technologies (DLTs) opens a wide range of possibilities for distributed security solutions, including the incorporation of reputation mechanisms and dynamic trust assessment. DLT has the potential of protecting the integrity of AI data via immutable records and distributed trust between different stakeholders. Additionally, smart contracts also open a range of opportunities for network applications that require peer-to-peer trustworthy interactions, as long as their verifiability can be supported by standardized methods.

Current cryptographic methods and protocols, rooted at the computational complexity of solving certain mathematical problems, are threatened by the advent of quantum computers. Several solutions are in progress to address this issue, with ongoing standardization activities that should be incorporated in future edge computing practice. Post-quantum cryptography (PQC), or quantum-resistant cryptography, aims for secure cryptographic systems against both quantum and classical computers. NIST is leading a standardization effort to make them interoperable with existing protocols and networks. Quantum cryptography follows a complementary approach, where a Quantum Key Distribution (QKD) system is nothing other than a source of synchronized random bits in two separated but connected locations. The ETSI ISG QKD is working on interfaces and operational procedures for integrating this technology within network operations and services.

References

The following documents are referenced in this text.

[ETSI-MEC] ETSI MEC, Multi-access Edge Computing (MEC), Link: https://www.etsi.org/technologies/multi-access-edge-computing

[ETSI-2014] ETSI GS NFV 002 - V1.2.1 - Network Functions Virtualisation (NFV); Architectural Framework. Retrieved from https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf

[MEC-003] ETSI GS MEC 003 V3.1.1 (2022-02): “Multi-access Edge Computing (MEC); Framework and Reference Architecture”, Link: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/03.01.01_60/gs_MEC003v030101p.pdf

[MEC-011] ETSI GS MEC 011 V2.2.1 (2020-12): “Multi-access Edge Computing (MEC); Edge Platform Application Enablement”, Link: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/011/02.02.01_60/gs_MEC011v020201p.pdf

[MEC-012] ETSI GS MEC 012 V2.2.1 (2022-02): “Multi-access Edge Computing (MEC); Radio Network Information API”, Link: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/012/02.02.01_60/gs_MEC012v020201p.pdf

[MEC-013] ETSI GS MEC 013 V2.2.1 (2022-01): “Multi-access Edge Computing (MEC); Location API”, Link: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/013/02.02.01_60/gs_MEC013v020201p.pdf

[MEC-030] ETSI GS MEC 030 V2.2.1 (2022-05): “Multi-access Edge Computing (MEC); V2X Information Service API”, Link: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/030/02.02.01_60/gs_MEC030v020201p.pdf

[MEC-009] ETSI GS MEC 009 V3.2.1 (2022-07): “Multi-access Edge Computing (MEC); General principles, patterns and common aspects of MEC Service APIs”, Link: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/009/03.02.01_60/gs_MEC009v030201p.pdf

[MEC-002] ETSI GR MEC 002 (2022-05): “Multi-access Edge Computing (MEC); Use Case and Requirements”

https://www.etsi.org/deliver/etsi_gs/MEC/001_099/002/02.02.01_60/gs_MEC002v020201p.pdf

[ETSIWP36] ETSI White Paper #36: “Harmonizing standards for edge computing - A synergized architecture leveraging ETSI ISG MEC and 3GPP specifications”, 1st edition – July 2020, Link: https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_wp36_Harmonizing-standards-for-edge-computing.pdf

[MEC-031] ETSI GR MEC 031 V2.1.1 (2020-10): “Multi-access Edge Computing (MEC) MEC 5G Integration”, Link: https://www.etsi.org/deliver/etsi_gr/MEC/001_099/031/02.01.01_60/gr_MEC031v020101p.pdf

[GSMA-PRD] GSMA Operator Platform Telco Edge Requirements, April 2022, Link: https://www.gsma.com/futurenetworks/wp-content/uploads/2022/04/GSMA-Operator-Platform-Telco-EdgeRequirements-2022-v2.0.pdf

[TS23.558] 3GPP TS 23.558, Architecture for enabling Edge Applications (EA), Link: https://www.3gpp.org/ftp/Specs/archive/23_series/23.558

[ENISA-5G] ENISA Threat Landscape for 5G Networks Report, Dec 2020, Link: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/

[SEC-013] ETSI GS NFV-SEC 013 V3.1.1 (2017-02): "Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification", Link: https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/013/03.01.01_60/gs_NFV-SEC013v030101p.pdf

[SEC-001] ETSI GS NFV-SEC 001 V1.1.1 (2014-10): "Network Functions Virtualisation (NFV); NFV Security; Problem Statement", Link: https://www.etsi.org/deliver/etsi_gs/nfv-sec/001_099/001/01.01.01_60/gs_nfv-sec001v010101p.pdf

[SEC-009] ETSI GS NFV-SEC 009 V1.1.1 (2015-12): "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration", Link: https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/009/01.01.01_60/gs_nfv-sec009v010101p.pdf

[SEC-012] ETSI GS NFV-SEC 012 V3.1.1 (2017-01): "Network Functions Virtualisation (NFV) - Release 3; Security; System architecture specification for execution of sensitive NFV components", Link: https://www.etsi.org/deliver/etsi_gs/nfv-sec/001_099/012/03.01.01_60/gs_nfv-sec012v030101p.pdf

[SEC-011] ETSI GR NFV-SEC 011 V1.1.1 (2018-04): "Network Functions Virtualisation (NFV); Security; Report on NFV LI Architecture", Link: https://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/011/01.01.01_60/gr_nfv-sec011v010101p.pdf

[SEC-010] ETSI GS NFV-SEC 010 V1.1.1 (2016-04): "Network Functions Virtualisation (NFV); NFV Security; Report on Retained Data problem statement and requirements", Link: https://www.etsi.org/deliver/etsi_gs/nfv-sec/001_099/010/01.01.01_60/gs_nfv-sec010v010101p.pdf

[SOL-013] ETSI GS NFV-SOL 013 V3.4.1 (2021-01): "Network Functions Virtualisation (NFV) Release 3; Protocols and Data Models; Specification of common aspects for RESTful NFV MANO APIs", Link: https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/013/03.04.01_60/gs_NFV-SOL013v030401p.pdf

[SEC-022] ETSI GS NFV-SEC 022 V2.8.1 (2020-06): "Network Functions Virtualisation (NFV) Release 2; Security; Access Token Specification for API Access", Link: https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/022/02.08.01_60/gs_NFV-SEC022v020801p.pdf

[SEC-023] Draft ETSI GS NFV-SEC 023 V0.0.4 (2020-07): " Network Functions Virtualisation (NFV); Security; Container Security Specification - Release 4", Link: https://docbox.etsi.org/ISG/NFV/Open/Drafts

[SEC-026] Draft ETSI GS NFV-SEC 026 V0.0.3 (2021-02): "Network Functions Virtualisation (NFV) Release 4; Security; Isolation and trust domain specification - Release 4 ", Link: https://docbox.etsi.org/ISG/NFV/Open/Drafts

[SEC-027] Draft ETSI GR NFV-SEC 027 V0.0.1 (2021-04): "Network Functions Virtualisation (NFV) Release 4; Security; Report on security assurance of NFVI - Release 4", Link: https://docbox.etsi.org/ISG/NFV/Open/Drafts

[TCG1] Trusted Computing Group, "TPM 2.0 Library Specification," Link: https://trustedcomputinggroup.org/resource/tpm-library-specification/

[ISO-15408] ISO/IEC 15408-1:2009: "Information technology, Security techniques, Evaluation criteria for IT security, Part 1: Introduction and general model.", Link: https://www.iso.org/standard/50341.html

[ISO-15408-2] ISO/IEC 15408-2:2022: "Information technology, Security techniques, Evaluation criteria for IT security, Part 2: Security functional components.", Link: https://www.iso.org/standard/72892.html

[TR33.839] 3GPP TR 33.839: "Study on security aspects of enhancement of support for edge computing in 5G Core (5GC)", Link: https://www.3gpp.org/ftp/specs/archive/33_series/33.839

[TR23.748] 3GPP TR 23.748: "Study on enhancement of support for Edge Computing in 5G Core network (5GC)"; Link: https://www.3gpp.org/ftp//Specs/archive/23_series/23.748

[TS23.548] 3GPP TS 23.548: "Study on application architecture for enabling Edge Applications", Link: https://www.3gpp.org/ftp/Specs/archive/23_series/23.548/

[TS23.758] 3GPP TS 23.758: "Study on application architecture for enabling Edge Applications", Link: https://www.3gpp.org/ftp/Specs/archive/23_series/23.758/

[TS23.558] 3GPP TS 23.558: "Architecture for enabling Edge Applications (EA)", Link: https://www.3gpp.org/ftp/Specs/archive/23_series/23.558/

[TS33.501] 3GPP TS 33.501: "Security architecture and procedures for 5G System", Link: https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/

[TR33.848] 3GPP TR 33.848: "Study on security impacts of virtualisation"; Link: https://ftp.3gpp.org//Specs/archive/33_series/33.848/

[TR33.818] 3GPP TR 33.818: "Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products"; Link: https://ftp.3gpp.org//Specs/archive/33_series/33.818/

[TS33.127] 3GPP TS 33.127: "Lawful Interception (LI) architecture and functions"; Link: https://ftp.3gpp.org//Specs/archive/33_series/33.127/

[TS33.558] 3GPP TS 33.558: "Security aspects of enhancement of support for enabling edge applications"; Link: https://ftp.3gpp.org//Specs/archive/33_series/33.558/

[TR33.739] 3GPP TR 33.739: "Study on security enhancement of support for edge computing phase 2"; Link: https://ftp.3gpp.org//Specs/archive/33_series/33.739/

[NESAS-2.0] Network Equipment Security Assurance Scheme – Overview; Version 2.0", 05 February 2021, Link: https://www.gsma.com/security/wp-content/uploads/2021/02/FS.13-NESAS-Overview-v2.0.pdf

[EU-NIS] Directive on security of network and information systems (NIS Directive); Link: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[EUCS2020] EUCS candidate scheme (European Cybersecurity Certification Scheme for Cloud Services); Dec 2020; Link: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

[EN303645] Draft ETSI EN 303 645 V2.1.0 (2020-04): "Cyber Security for Consumer Internet of Things: Baseline Requirements", Link: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf

[TS103701] Draft ETSI TS 103 701 V0.0.7 (2021-03): "Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements", Link: https://docbox.etsi.org/CYBER/CYBER/Open/Latest_Drafts/CYBER-0050v007-TS103701-Cybersecurity-assessment-for-consumer-IoT-product.pdf

[TS103486] Draft ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT", DTS/CYBER-0014' Work Item: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=47653

[TS103742] Draft ETSI TS 103 742: "CYBER; Baseline Cybersecurity for a Communications Network", DTS/CYBER-0055' Work Item: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58919

[SASE2019] Gartner, "The Future of Network Security Is in the Cloud'", published 13 September 2019, Link: https://www.gartner.com/en/documents/3957375

ETSI The Standards People

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org