ETSI GR MEC 041 V3.1.1 (2024-03)

Multi-access Edge Computing (MEC); Study on MEC Security

Disclaimer

The present document has been produced and approved by the Multi-access Edge Computing (MEC) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/MEC-0041v311MECSecurity

Keywords
application, MEC, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 6
3 Definition of terms, symbols and abbreviations 8
3.1 Terms 8
3.2 Symbols 8
3.3 Abbreviations 8
4 Overview 8
4.1 Introduction 8
4.2 Platform and Software Security 8
4.3 Zero-Trust Architecture 9
4.4 Trusted Computing and Attestation 9
4.5 Security Monitoring and Management 9
4.6 MEC Federations 10
4.7 MEC architecture and security 11
4.7.1 Description 11
4.7.2 Authentication 11
4.7.3 Authorization 11
5 Key issues and potential solutions 12
5.1 Key issue #1: Stolen MEC App access tokens 12
5.1.1 Description 12
5.1.2 Solution proposal #1: Adopt OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens 13
5.1.2.1 Description 13
5.1.2.2 Configure client credentials 13
5.1.2.3 OAuth Client registration and access token 13
5.1.2.4 Authorizing access to MEC Services 14
5.1.3 Evaluation 15
5.2 Key issue #2: Stolen MEC App identity 15
5.2.1 Description 15
5.2.2 Solution proposal #1: Enhance MEC App Authentication using hardware-based security 16
5.2.2.1 Description 16
5.2.2.2 Generating Client Credentials bound to the RoT entity 16
5.2.2.3 OAuth Client registration and access token 17
5.2.2.4 Authorizing access to MEC Services 18
5.2.3 Evaluation 18
5.3 Key issue #3: Compromised MEC applications, asset theft 19
5.3.1 Description 19
5.3.2 Solution proposal #1: Verify provenance of MEC applications through cryptographic attestations 20
5.3.2.1 Description 20
5.3.2.2 Assessing trustworthiness of MEC applications 21
5.3.2.3 Attestation framework for MEC applications 22
5.3.3 Solution proposal #2: Verify integrity of MEC applications through cryptographic attestation 23
5.3.3.1 Description 23
5.3.3.2 Solution Details 24
5.3.4 Solution proposal #3: Continuous verification of integrity of MEC applications through periodic attestation 25
5.3.4.1 Description 25
5.3.4.2 Solution Details 25
5.3.5 Evaluation 25

5.4 Key issue #4: Compromise of application package during on-boarding 26
5.4.1 Description 26
5.4.2 Solution proposal #1: Secure onboarding of MEC application packages 27
5.4.2.1 Description 27
5.4.2.2 Solution details 27
5.4.3 Evaluation 28
5.5 Key issue #5: Compromise of application during updates 28
5.5.1 Description 28
5.5.2 Solution proposal #1: Secure MEC Application Update 29
5.5.2.1 Description 29
5.5.2.2 Solution details 29
5.5.3 Evaluation 30
5.6 Key issue #6: Threats associated with Application Package Deletion 30
5.6.1 Description 30
5.6.2 Solution proposal #1: Secure application package deletion 31
5.6.2.1 Description 31
5.6.2.2 Solution details 32
5.6.3 Evaluation 32
5.7 Key issue #7: MEC App anomalous behaviour 32
5.7.1 Description 32
5.7.2 Solution proposal #1: Security Monitoring and Management for MEC 33
5.7.2.1 Description 33
5.7.2.2 Solution details 35
5.7.3 Evaluation 35
6 Gap analysis and recommendations 35
Annex A: Change History 37
History 38

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Multi-access Edge Computing (MEC).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document outlines security topics and paradigms that apply to MEC deployments across the realms of application/platform security and zero-trust architecture. The present 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.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR MEC 001: "Multi-access Edge Computing (MEC); Terminology".

[i.2] ETSI GR MEC 035: "Multi-access Edge Computing (MEC); Study on Inter-MEC systems and MEC-Cloud systems coordination".

[i.3] CNCF: "Cloud Native Computing Foundation".

[i.4] NIST SP 800-207: "Zero Trust Architecture", August 2020.

[i.5] SDP Specification 1.0: "Software Defined Perimeter", Cloud Security Alliance (2015).

[i.6] ETSI White Paper No. 46: "MEC security: Status of standards support and future evolutions", 2nd edition - September 2022.

[i.7] TCG: "Trusted Computing Group".

[i.8] IETF RFC 9334: "Remote Attestation Procedures".

[i.9] GSMA White Paper: "Operator Platform Telco Edge Proposal", Oct. 2020.

[i.10] GSMA OPG.02: "Operator Platform: Requirements and Architecture"; Version 5.0, 26th July 2023.

[i.11] ETSI GS MEC 003: "Multi-access Edge Computing (MEC); Framework and Reference Architecture".

[i.12] ETSI GS MEC 009: "Multi-access Edge Computing (MEC); General principles, patterns and common aspects of MEC Service APIs".

[i.13] Trusted Platform Module Library: "Part 1: Architecture".

[i.14] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[i.15] IETF RFC 8705: "OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens".

[i.16] IETF RFC 7591: "OAuth 2.0 Dynamic Client Registration Protocol".

[i.17] IETF RFC 2986: "PKCS #10: Certification Request Syntax Specification Version 1.7".

[i.18] IETF CoRIM: "Concise Reference Integrity Manifest".

[i.19] NTIA SBOM: "SBOM at a glance".

[i.20] 3GPP TR 33.848: "Study on Security Impacts of Virtualisation", Version 18.0.0.

[i.21] ETSI GS NFV-SEC 012: "System architecture specification for execution of sensitive NFV components", Version 3.1.1.

[i.22] IETF draft-fossati-tls-attestation: "Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)".

[i.23] TCG: "DICE Endorsement Architecture for Devices", Version 1.0, Revision 0.38.

[i.24] IETF draft-sandowicz-httpbis-httpa2: "The Hypertext Transfer Protocol Attestable (HTTPA) Version 2".

[i.25] Linux IMA: "Integrity Measurement Architecture".

[i.26] NIST SP 800-218: "Secure Software Development Framework (SSDF) Version 1.1", February 2022.

[i.27] ISO/IEC 5962:2021: "Software Package Data Exchange".

[i.28] SLSA: "Supply chain Levels for Software Artifacts".

[i.29] OWASP CycloneDX: "Lightweight Bill of Materials (BOM) standard".

[i.30] ETSI GS MEC 010-2: "Multi-access Edge Computing (MEC); MEC Management; Part 2: Application lifecycle, rules and requirements management".

[i.31] ETSI GS NFV-SEC 013: "Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification".

[i.32] 3GPP TR 33.894: "Study on zero-trust security principles in mobile networks", Version 18.0.0.

[i.33] Cloud Security Alliance: "Cloud Controls Matrix", Version 3.0.1.

[i.34] GSMA: "FS.31 GSMA Baseline Security Controls", Version 2.0.

[i.35] ETSI GS NFV-SEC 013: "Network Functions Virtualisation (NFV) Release 3; Security ; Security Management and Monitoring specification".

[i.36] ETSI GS NFV-SEC 024: "Network Functions Virtualisation (NFV) Security; Security Management Specification".

[i.37] TCG DICE: "Device Identifier Composition Engine", Level 00 Revision 78.

[i.38] TCG DICE-Layering: "DICE Layering Architecture", Version 1.0, Revision 0.19.

[i.39] W3CDID: "Decentralized Identifiers", Version 1.0.

[i.40] ETSI GS MEC 011: "Multi-access Edge Computing (MEC); Edge Platform Application Enablement".

[i.41] ETSI GS MEC 002: "Multi-access Edge Computing (MEC); Use Cases and Requirements".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GR MEC 001 [i.1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR MEC 001 [i.1] and the following apply:

AA	Authentication and Authorization
CNCF	Cloud Native Computing Foundation
CSP	Cloud Service Provider
DoS	Denial of Service
DDoS	Distributed Denial of Service
RoT	Root of Trust
SMM	Security Monitoring and Management
TEE	Trusted Execution Environment
ZTA	Zero-Trust Architecture

4 Overview

4.1 Introduction

The present document outlines security topics and paradigms that apply to MEC deployments across the realms of App/platform security and zero-trust architecture.

The present clause introduces the MEC security landscape, with reference to current initiatives in the field. Clause 5 documents key issues that illustrate security challenges in MEC systems to analyse gaps in the current ETSI MEC specifications. Clause 6 summarizes the recommendations from clause 5 for closing those gaps. The present document considers prior work of other industry/standards bodies as well as all relevant work done in ETSI.

4.2 Platform and Software Security

Edge computing platforms are often located outside physical security zones typical for data centres. This makes the critical importance of platform integrity [i.6] an increasingly top-of-mind issue for edge cloud architects. ETSI ISG MEC needs to be able to address questions around whether platform integrity needs to play a role in processes such as App LCM and if so, what that role is and what, if any, API enhancements are needed to enable it.

Further, edge deployments constitute a complex multi-vendor, multi-supplier, and multi-stakeholder ecosystem lacking a central entity that implements system-wide security assurances or accepts full liability if things go wrong. Software assets from these various parties along with their user's data are under threat of IP theft, ransomware attacks or Denial of Service (DoS) attacks. ETSI MEC specifications could thus draw upon threat mitigation strategies and practices currently employed by major Cloud Service Providers (CSPs) and/or driven by the Cloud Native Computing Foundation (CNCF) [i.3].

4.3 Zero-Trust Architecture

The migration towards cloud-native implementations of both Apps and network functions combined with the highly distributed and multi-tenant nature of distributed clouds is increasingly driving adoption of Zero-Trust Architecture (ZTA) [i.4] concepts such as Software Defined Perimeter [i.5]. Because ZTA is premised on validating trust on each and every cloud entity (e.g. App instance), it is not unreasonable to expect that adoption of ZTA may impact MEC App LCM operations, which may require additional API standardization.

4.4 Trusted Computing and Attestation

Trusted computing technologies uphold consistent behaviour of computing systems (e.g. MEC Hosts) by ensuring that their underlying components are unmodified and not executing unauthorized or malicious code. This is achieved during the boot process by certifying the provenance of firmware and successive levels of the software stack through a chain of trust originating at a root of trust. The Trusted Computing Group (TCG) [i.7] specifications outline the requirements and cryptographic constructions for implementing trusted computing as a vendor-neutral standard.

Attestation is the process of creating, conveying, and appraising the trustworthiness characteristics of a computing system. This is accomplished through *Attester* and *Verifier* roles in a scenario where a *Relying Party* (e.g. API endpoint) assesses the trustworthiness of another computing entity (e.g. API requester). The Verifier may reside on (for example) the API backend and the Attester on (for example) the API requester. The Relying Party, typically, issues a challenge request to the Attester for a specific scope of the API requester's characteristics. Integrity measurements (e.g. digests) of system software components (e.g. firmware, kernel modules) from the API requester's environment may be compiled into *Attestation Evidence* by an Attester and presented to a Verifier. The Verifier authenticates the received Attestation Evidence and compares it to known good values previously delivered to the Verifier to arrive at a verdict on the trustworthiness of the attesting system and its software stack. Typically, the Attester is constructed with a root of trust that is implicitly trusted, that is to say, trust in the root of trust is vouched for by its manufacturer by issuing a certificate or other endorsement document that describes the root of trust technology. Typically, a root of trust is implemented using tamper-resistant technology (see [i.37]). A trustworthy Attester typically has bootstrapped trusted modules that are inspected by the root of trust or a delegate trusted module, see [i.38]. Further, trust relationships between the entities that implement attestation roles, e.g. Attester, Verifier and Relying Party, are typically established using Public Key Infrastructure (PKI) but alternatives are also possible, see [i.39].

IETF RFC 9334 [i.8] defines Attestation roles, conceptual messages, and patterns for message exchange that can be integrated into network protocols and APIs. The aim of attestation integration is to condition traditional data and control flow operations based on a trust assessment. Traditional message flow assumes the peers of a message exchange are implicitly trustworthy without performing a trust assessment.

The decentralized nature of cloud-based, virtualized architectures has made it easier for firmware and kernel rootkits to cause privilege escalation and exfiltrate data. Popular CSPs may rely on trusted computing technology in their infrastructures to detect and eliminate such attacks. As MEC deployments are subject to similar attack vectors, it may be useful for MEC designers to consider adoption of trusted computing methodologies for future MEC standards.

4.5 Security Monitoring and Management

Security Monitoring and Management (SMM) refers to activities undertaken by network operators or communication service providers employing a set of tools and mechanisms to continually preserve the security of their network deployment (physical, virtualized or hybrid).

In particular, security monitoring involves using passive or active probing of traffic flows on the user data, control, or management planes, and extracting statistics of infrastructure usage (network, compute, storage) of the network components. At a higher level, security monitoring can involve inspection of network entity state and message flows between network entities. Importantly, security monitoring has to lead to a view over the entire network (virtual and physical).

Security management on the other hand involves two aspects: the establishment of security policies, and the enforcement of these policies. Notably, there is a processing of the data gathered from the security monitoring tools, often aided by AI/ML and data analytics. In addition, the enforcement of policies involves mainly automated (as opposed to human-decision-driven) security management actions. Numerous tools exist commercially for both security monitoring and management (separately or bundled together).

Security monitoring and management systems can help to ensure platform and software security (clause 4.2) of the MEC platform and other MEC components. A SMM system employs behavioural monitoring (also referred to as telemetry) to identify MEC entities acting outside expectations for proper and secure operation. Once identified, the SMM system can take steps to limit the operation (and hence potential incurred damage) of the identified MEC entity.

In support of SMM, MEC data collection and processing is a key activity, e.g. logging of all security events experienced by a MEC App, MEC host, MEC Platform, and other MEC components. Collection and processing of such data can be done in an efficient but secure fashion with privacy considerations in mind, and the logs can be access-controlled to prevent unauthorized modification and ensure accuracy of subsequent auditing or forensics activities. Anomalies found in collected security-related data could indicate a malfunction or a security incident (e.g. malware has been activated).

For security management, a security manager entity will take action in response to a suspect incident, behaviour or activity.

The SMM for a MEC system SMM can be defined so as to integrate with existing tools being used in the operator networks, such as Network Intrusion Detection Systems (NIDS), Network Intrusion Prevention Systems (NIPS) and deep packet inspection firewalls. Operators manage complex networks and use a variety of tools to undertake their SMM activities. The industry and standards bodies have not produced a unified SMM authoritative framework or general usage document, but best practices and guidance exist, allowing the operators to select and customize the set of tools to fit their own business objectives. Therefore, a MEC system, once added to an existing network, can provide the requisite security monitoring telemetry feeds and allow for security management actions to be taken in response, based on policies defined by each operator.

Other industry forums and SDOs have laid out some best practices and high-level measures for security monitoring and/or management (e.g. it is part of Zero Trust currently under study in 3GPP TR 33.894 [i.32], part of the "Cloud Control Matrix v3.0.1" [i.33] in the Cloud Security Alliance, and part of FS.31 Baseline Security Controls v2.0 [i.34] in GSMA). In particular, SMM for NFV systems is specified in ETSI GS NFV-SEC 013 [i.31], with the goal to establish the NFV Security Lifecycle Management and Security Monitoring requirements and architecture. Some elements of the ETSI NFV-SEC defined SMM can be re-used for ETSI MEC (where applicable). These can be taken into account by a MEC system operator when defining the particular profiles and policies for the various MEC entities and integrate them into their existing network management tools.

4.6 MEC Federations

ETSI MEC is introducing architectural enhancements to enable a federation of MEC systems [i.2], allowing for inter-MEC system communications in scenarios involving multiple MNOs. This is a use case where security is a critical requirement from operators and all federating entities. Each MNO establishes and administers its own security domain that should remain isolated from the security domains of other MNOs.

The GSMA Operator Platform Group (GSMA OPG) has defined the notion of an Operator Platform (OP) [i.9], [i.10] as the entity that mediates access to the edge cloud capabilities of an MNO. The GSMA further stipulates that OP instances implement the East/West Bound Interface (E/WBI) between MNOs where the OP abstracts away the internal topology and configuration of the MNO. For this purpose, GSMA OPG introduces a Common Data Model (CDM) to describe characteristics of the elements of an OP instance, including OP roles, applications, edge clouds, and security. The GSMA OPG requirements as inferred from [i.9] suggest the ability to identify clients, application providers and applications, along with encrypted and authorized access to edge resources across federated OP instances.

As ETSI MEC is considering GSMA OPG requirements for realizing MEC Federations, the security aspects of OP architecture and related MEC implications are to be carefully considered. In particular, MEC security can be studied from the perspective of edge cloud services through an analysis of its threat models and providing solutions for managing identity, authentication and authorization of client and edge applications across edge clouds via their OP instances.

4.7 MEC architecture and security

4.7.1 Description

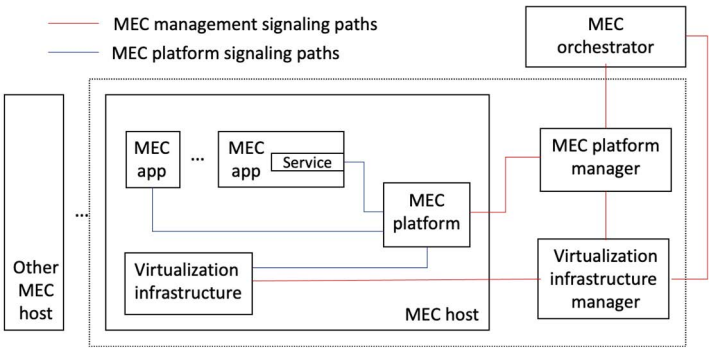


Figure 4.7.1-1: Multi-access edge system

Figure 4.7.1-1 is a simplified depiction of the MEC reference architecture that is documented in ETSI GS MEC 003 [i.11]. A MEC system broadly consists of MEC hosts and management elements to support MEC applications. MEC applications are software-only entities that execute in Virtual Machines (VM) or containers over a virtualization infrastructure that is situated close to end-users of the applications.

A MEC host is a physical entity that contains a MEC platform and the virtualization infrastructure. MEC management operates through the MEC platform to configure the deployment of MEC applications to the virtualization infrastructure and to aid them throughout their lifecycle.

MEC management at the system-level includes the MEC Orchestrator (MEO) which maintains a view of the whole MEC system. The MEO onboards application packages, performs integrity checks, and selects an appropriate MEC host to deploy the application.

MEC management at the host-level includes the MEC Platform Manager (MEPM) and the Virtualization Infrastructure Manager (VIM). The MEPM serves as the control plane for the MEC platform and is a conduit to the MEO. The VIM is responsible for allocating, managing, and releasing virtualized (computing, storage, and networking) resources of the virtualization infrastructure.

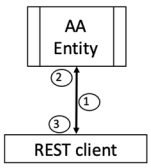
ETSI GS MEC 009 [i.12] describes patterns for authentication and authorization of MEC applications over RESTful and alternate transports that are summarized below in clauses 4.7.2 and 4.7.3. These patterns also apply to the NFV variant of the MEC reference architecture specified in ETSI GS MEC 003 [i.11].

4.7.2 Authentication

MEC specifications mandate HTTPS support in all RESTful MEC service APIs using TLS v1.2 or TLS v1.3 and prohibit the use of HTTP without TLS or TLS versions preceding v1.2. TLS secures the transmission channel between peers. During the TLS handshake, peers may mutually authenticate themselves using X.509 certificates that follow a chain of trust to a trusted Certificate Authority.

4.7.3 Authorization

Authorization to access RESTful MEC service APIs defined by ETSI ISG MEC is achieved using the OAuth 2.0 protocol [i.14]. The MEC specifications posit an Authentication and Authorization (AA) entity that is accessible to both the REST client and server. A trusted manager entity configures the AA entity with appropriate credentials and REST clients' access rights to server resources. REST clients further authenticate to the AA entity to request an access token using the OAuth client credentials grant.



1. REST client initiates a HTTPS session with the AA entity
2. REST client issues a request to its OAuth token endpoint providing its client secret
3. The AA entity returns an access token to the Client

Figure 4.7.3-1: Acquiring an access token using OAuth 2.0

REST clients present this token in requests to resources hosted in REST servers over an authenticated HTTPS session. On receiving a request, REST servers may communicate with the AA entity to authorize the request before returning a response.