ETSI GS MEC 062 V4.1.1 (2026-02)

GROUP SPECIFICATION

Multi-access Edge Computing (MEC); Support for Security Monitoring and Management

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
DGS/MEC-0062v411SMM

Keywords
cybersecurity, MEC, network monitoring

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

Contents

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Multi-access Edge Computing (MEC).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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 specifies the information flows, security-related data for collection, and as applicable, specifies the necessary data model and format needed to support the Security Monitoring and Management (SMM) feature for the MEC system.

The present document also provides guidance on other aspects of SMM, including security profiles, security directives, security policies, and the functionality related to the collection, distribution, and storage of security data.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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 necessary for the application of the present document.

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

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

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

Not applicable.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AA	Authentication and Authorization
API	Application Programming Interface
CPU	Central Process Unit
DNS	Domain Name System
HTTP	HyperText Transfer Protocol
SMM	Security Monitoring and Mnaagement
SMMF	Security Monitoring and Management Function

4 Overview

The present document specifies aspects of the Security Monitoring and Management Function (SMMF) and Ms reference points in support of SMM for the MEC system and the corresponding requirements defined in clause 6.3.15 of ETSI GS MEC 002 [1].

Clause 5 introduces the functionalities enabled via the Ms interfaces. It provides the high level information flows and describes the necessary operations. The data model is defined in clause 6.

5 Description of the service (informative)

5.1 Introduction

Network operators or communications service providers may undertake activities employing a set of tools and mechanisms to maintain the security of their network deployment (physical, virtualized or hybrid). MEC system support for Security Monitoring and Management (SMM) can be realized through the Feature SMM in ETSI GS MEC 002 [1], and this support is described in the present document.

When supporting the Feature SMM, the MEC system can provide MEC-specific security-related data monitoring and means for the ensuing security management. Existing SMM systems can gather security-related data from the MEC system. Additionally, the MEC SMM Function (SMMF) and Ms interfaces can be optionally implemented to offer more comprehensive MEC-related SMM support if needed. The SMMF can be managed by OSS.

The operation of MEC-specific SMM can be described using the following basic components:

- Security Alert: notification that a security event has occurred in the MEC system as determined by the SMM system based upon analysis of collected monitoring data.
- Security Profile: A set of security-related data a MEC entity can deliver to the SMM system as well as what security directives it will respond to and how.
- Security Directive: A set of actions a MEC entity can perform in response to a security alert notification.
- Control Policy: A control policy determines the actions to be taken (security directive) by MEC entities in response to a security alert.
- Monitoring Policy: A monitoring policy specifies parameters such as data collection, analysis, and alerts.

5.2 Sequence Diagrams

5.2.1 General

The following clauses describe how SMMF may be supported by the MEC platform via Ms reference points. The related sequence diagrams are presented.

Table 5.2.1-1 maps the message flows in clause 5.2 to the applicable reference point(s) as defined in clause 7.2.6 of ETSI GS MEC 003 [2] and data type(s) in clause 6 of the present document.

Table 5.2.1-1: Message flow mapping to applicable reference point(s) and data type(s)

Message Flow	Applicable Reference Point(s)	Applicable Info Model Data Type(s)
5.2.2 Activation of SMM	Ms1	Implementation specific
5.2.3 Deactivation of SMM	Ms1	Implementation specific
5.2.4 Activation of SMM control policy	Ms1	ControlPolicy (clause 6.2.5)
5.2.5 Deactivation of SMM control policy	Ms1	ControlPolicy (clause 6.2.5)
5.2.6 Activation of SMM monitoring policy	Ms1	SourcesMonitoringPolicy (clause 6.2.2), AnalysisMonitoringPolicy (clause 6.2.3), AlertsMonitoringPolicy (clause 6.2.4)
5.2.7 Deactivation of SMM monitoring policy	Ms1	SourcesMonitoringPolicy (clause 6.2.2), AnalysisMonitoringPolicy (clause 6.2.3), AlertsMonitoringPolicy (clause 6.2.4)
5.2.8 Security directive notification	Ms1	SecurityDirective (clause 6.4.2)
5.2.9 Security alert notification	Ms1	SecurityAlert (clause 6.5.2)
5.2.10 Monitoring Profile Request	Ms2, Ms3, Ms4, Ms5	MonitoringProfile (clause 6.3.2)
5.2.11 Data monitoring subscription	Ms2, Ms3, Ms4, Ms5	Implementation specific
5.2.12 Data monitoring unsubscribe	Ms2, Ms3, Ms4, Ms5	Implementation specific
5.2.13 Data query	Ms2, Ms3, Ms4, Ms5	Implementation specific
5.2.14 Directive Profile Request	Ms2, Ms3, Ms4, Ms5	DirectiveProfile (clause 6.3.3)
5.2.15 Security Directive Notification	Ms2, Ms3, Ms4, Ms5	SecurityDirective (clause 6.4.2)
5.2.16 Send Data	Ms2, Ms3, Ms4, Ms5	Implementation specific

5.2.2 Activation of SMM

Figure 5.2.2-1 shows the message flow for activating SMM.

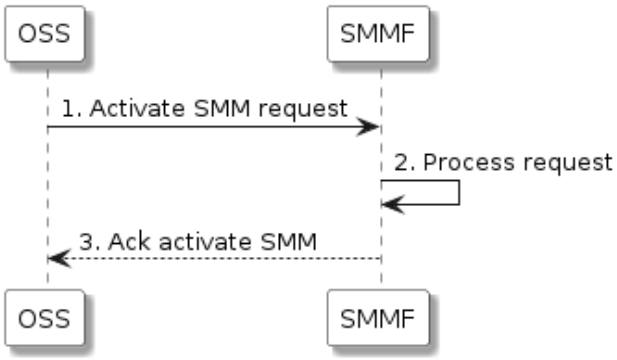

Figure 5.2.2-1: SMM Activation Flow

1) The OSS sends an SMM activation request to the SMMF.
2) The SMMF processes the request of SMM activation. If SMM is disabled, the SMMF activates it.
3) The SMMF sends to the OSS an acknowledgment to the SMM activation request.

5.2.3 Deactivation of SMM

Figure 5.2.3-1 shows the message flow for deactivating SMM.

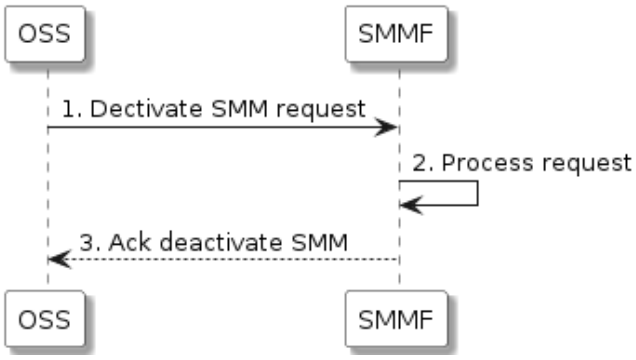

Figure 5.2.3-1: SMM Deactivation Flow

1) The OSS sends an SMM deactivation request to the SMMF.
2) The SMMF processes the request of SMM deactivation. If SMM is enabled, the SMMF deactivates it.
3) The SMMF sends to the OSS an acknowledgment to the SMM deactivation request.

5.2.4 Activation of SMM control policy

Figure 5.2.4-1 shows the message flow for activating SMM control policy.

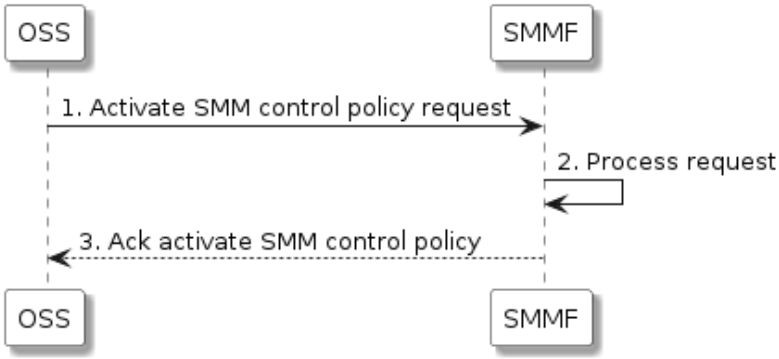

Figure 5.2.4-1: SMM control policy activation flow

1) The OSS sends an SMM control policy activation request to the SMMF.
2) The SMMF processes the request of SMM control policy activation. If the requested SMM control policy is not active, the SMMF activates it.
3) The SMMF sends to the OSS an acknowledgment to the SMM control policy activation request.

NOTE: There can be only one active SMM control policy at a time.

5.2.5 Deactivation of SMM control policy

Figure 5.2.5-1 shows the message flow for deactivating SMM control policy.

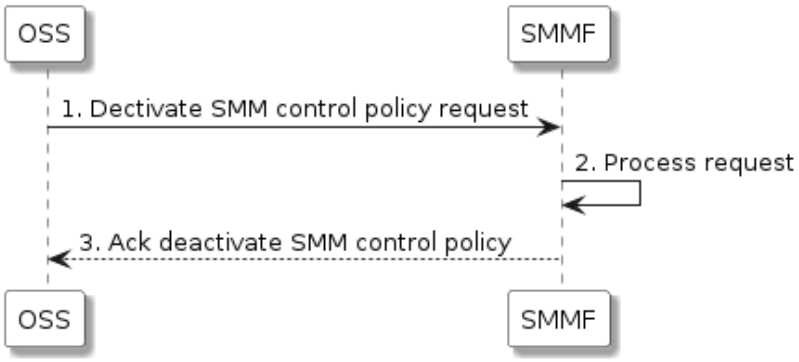

Figure 5.2.5-1: SMM control policy deactivation flow

1) The OSS sends an SMM control policy deactivation request to the SMMF.

2) The SMMF processes the request of SMM deactivation. If the requested SMM control policy is active, the SMMF deactivates it.

3) The SMMF sends to the OSS an acknowledgment to the SMM control policy deactivation request.

5.2.6 Activation of SMM monitoring policy

Figure 5.2.6-1 shows the message flow for activating SMM monitoring policy.

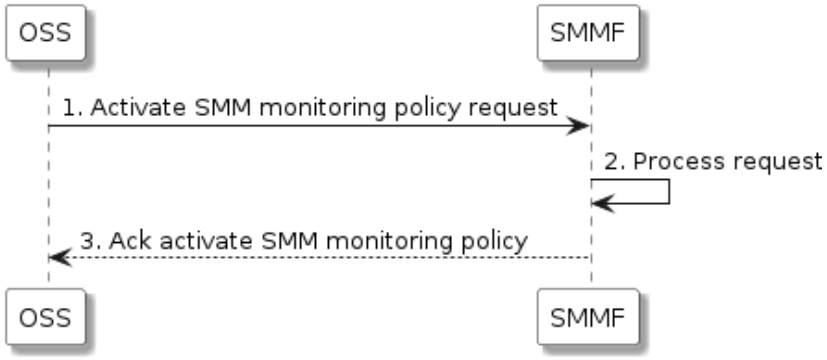

Figure 5.2.6-1: SMM monitoring policy activation flow

1) The OSS sends an SMM monitoring policy activation request to the SMMF.

2) The SMMF processes the request of SMM monitoring policy activation. If the SMM monitoring policy is not active, the SMMF activates it.

3) The SMMF sends to the OSS an acknowledgment to the SMM monitoring policy activation request.

5.2.7 Deactivation of SMM monitoring policy

Figure 5.2.7-1 shows the message flow for deactivating SMM monitoring policy.

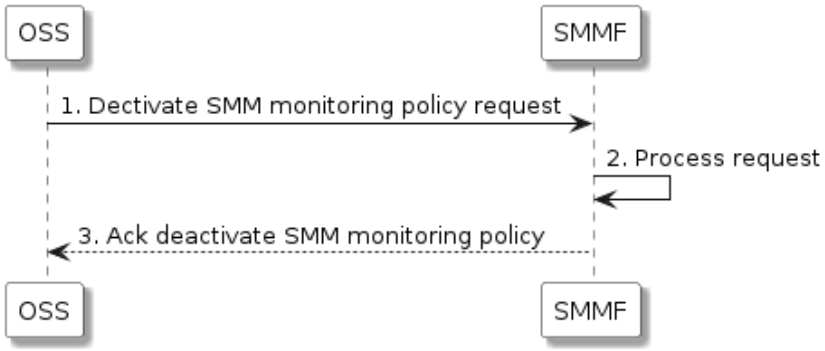

Figure 5.2.7-1: SMM monitoring policy deactivation flow

1) The OSS sends an SMM monitoring policy deactivation request to the SMMF.
2) The SMMF processes the request of SMM deactivation. If the SMM monitoring policy is active, the SMMF deactivates it.
3) The SMMF sends to the OSS an acknowledgment to the SMM monitoring policy deactivation request.

5.2.8 Security directive notification

Figure 5.2.8-1 shows the message flow for a security directive notification from SMMF to OSS.

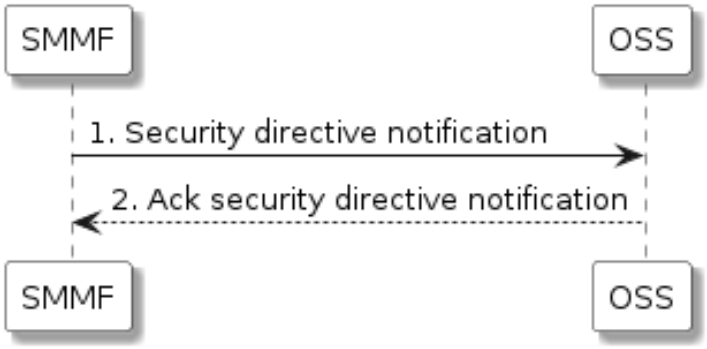

Figure 5.2.8-1: Security directive notification flow

1) The SMMF sends notification to the OSS of each generated security directive sent to a MEC entity.
2) The OSS responds with an acknowledgement to the security directive notification.

5.2.9 Security alert notification

Figure 5.2.9-1 shows the message flow for a security alert notification from SMMF to OSS.

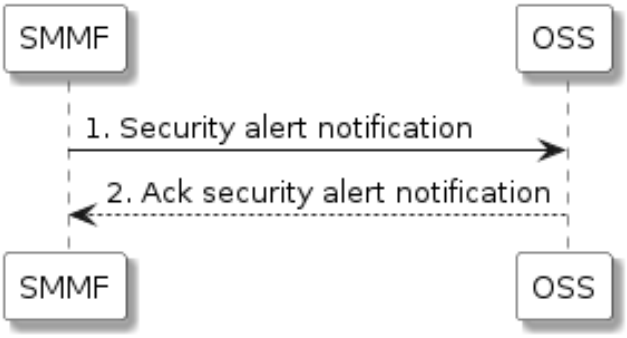

Figure 5.2.9-1: Security alert notification flow

1) The SMMF sends a notification to the OSS of each security alert received from a MEC entity.

2) The OSS responds with an acknowledgement to the security alert notification.

5.2.10 Monitoring Profile Request

Figure 5.2.10-1 shows the message flow for a monitoring profile request.

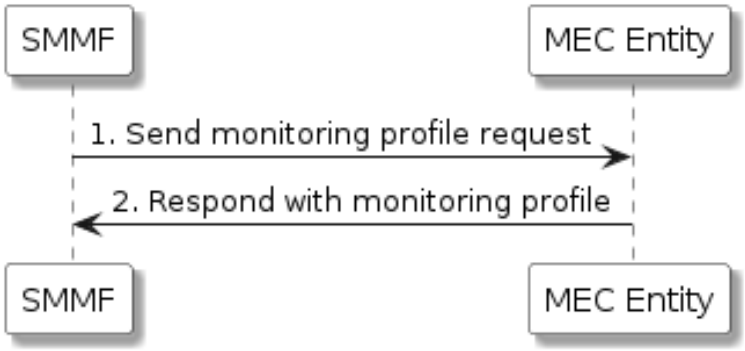

Figure 5.2.10-1: Monitoring profile request flow

1) The SMMF sends a request for the MEC entity's monitoring profile.

2) The MEC entity responds with its monitoring profile to SMMF.

5.2.11 Data monitoring subscription

Figure 5.2.11-1 shows the message flow for a data monitoring subscription.

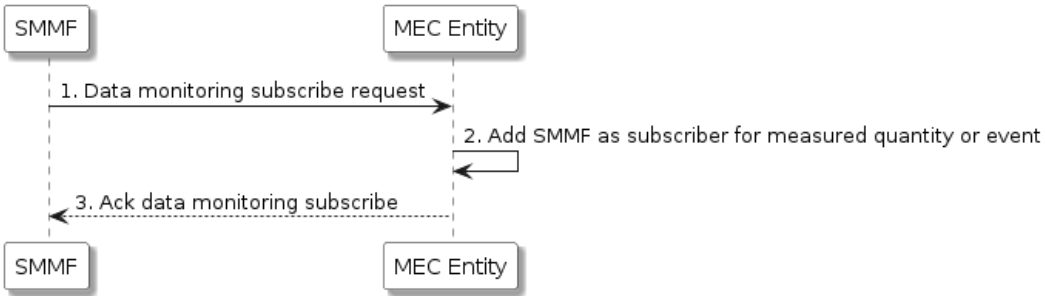

Figure 5.2.11-1: Data monitoring subscription flow

1) The SMMF sends a request to subscribe to a measured quantity or event that a MEC entity observes.

2) The MEC entity adds SMMF as subscriber for the measured quantity or event.

3) The MEC entity responds with an acknowledgement to the data monitoring subscription request.

5.2.12 Data monitoring unsubscribe

Figure 5.2.12-1 shows the message flow for a data monitoring unsubscribe request.

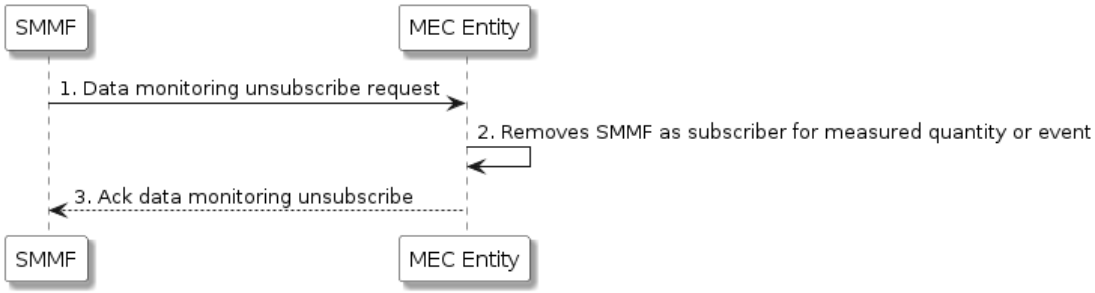

Figure 5.2.12-1: Data monitoring unsubscribe flow

1) The SMMF sends a request to unsubscribe to a measured quantity or event that a MEC entity observes.
2) The MEC entity removes SMMF as subscriber for the measured quantity or event.
3) The MEC entity responds with an acknowledgement to the data monitoring unsubscribe request.

5.2.13 Data query

Figure 5.2.13-1 shows the message flow for a data query request.

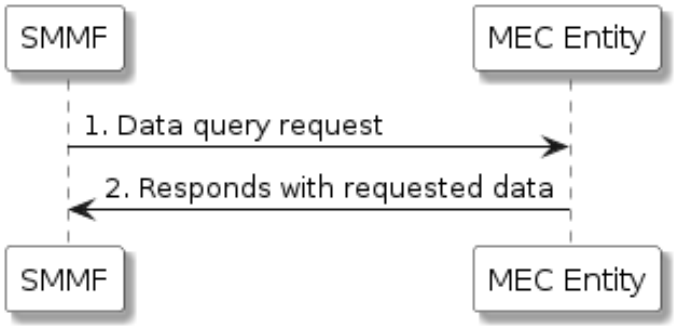

Figure 5.2.13-1: Data query request flow

1) The SMMF sends a request for the most recent data a MEC entity collects.
2) The MEC entity sends the requested data to the SMMF.

5.2.14 Directive Profile Request

Figure 5.2.14-1 shows the message flow for a directive profile request.

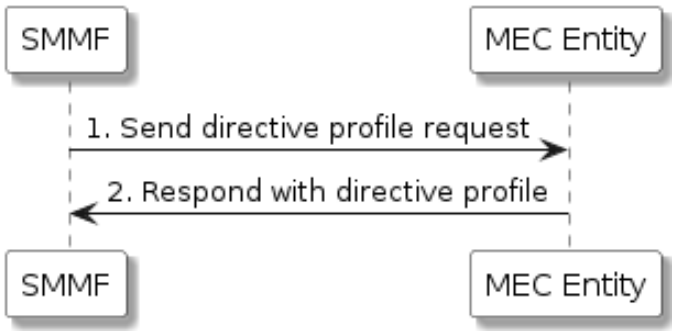

Figure 5.2.14-1: Directive profile request flow

1) The SMMF sends a request for the MEC entity's security directive profile.
2) The MEC entity sends its security directive profile to SMMF.

5.2.15 Security Directive Notification

Figure 5.2.15-1 shows the message flow for a security directive notification from SMMF to MEC entity.

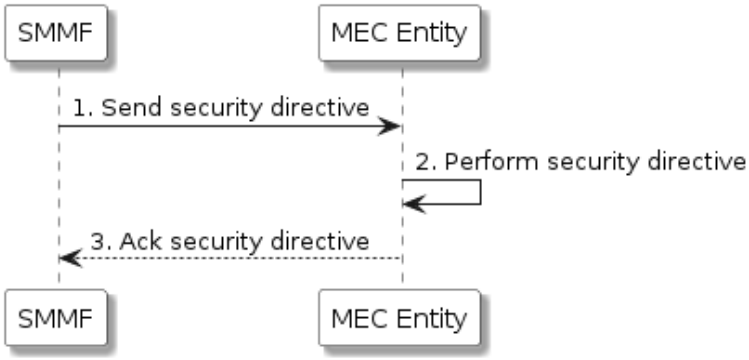

Figure 5.2.15-1: Security directive notification flow

1) The SMMF sends a security directive notification to a MEC entity.
2) The MEC entity performs the security directive.
3) The MEC entity responds with an acknowledgement to the security directive notification.

5.2.16 Send Data

Figure 5.2.16-1 shows the message flow for sending data.

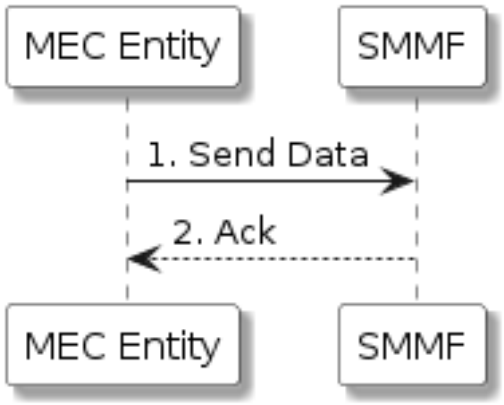

Figure 5.2.16-1: Send data flow

1) The MEC entity sends data to the SMMF as subscribed by the SMMF in clause 5.2.11.
2) The SMMF responds with an acknowledgement.

6 Information Model

6.1 Introduction

The following clauses specify the information model that is to be used for the Ms interfaces and the information flows specified in clause 5. It may also be used in operator implementations of SMM systems. This information model, which can be extended as necessary, is the minimum normative specification for this optional feature. The actual nomenclature in the following data types is not prescriptive. However, a compliant SMM implementation should map to this information model.

NOTE: In the following tables, N (which may be a different value in each instance) is an integer representing the maximum cardinality for the associated attribute.

6.2 Policy data types

6.2.1 Introduction

There are two types of policies: Monitoring and Control. Both policy types indicate the actions (and associated triggers) of the SMMF as defined for an SMM implementation. A monitoring policy specifies parameters pertinent to SMM operations such as data collection, analysis, and alerts. A control policy determines the actions that may be taken (security directive) by MEC entities due to a security alert generated by the SMMF.

6.2.2 Type: SourcesMonitoringPolicy

This type represents the data to be collected, frequency of collection, and source MEC entity.

Table 6.2.2-1: Attributes of SourcesMonitoringPolicy

Attribute name	Data type	Cardinality	Description
`policyId`	String	1	Identifies the monitoring policy.
`measuredEntity`	String	1	Identifies the MEC entity to which the data relates.
`measurementParameters`	STRUCT	1	Identifies the measurements to collect and corresponding periodicities, as well as events to monitor for.
NOTE: The measurementParameters attribute is described in clause 6.6.2.			

6.2.3 Type: AnalysisMonitoringPolicy

This type indicates to the SMMF the analyses to be conducted, including the required inputs and frequency.

Table 6.2.3-1: Attributes of AnalysisMonitoringPolicy

Attribute name	Data type	Cardinality	Description
`policyId`	String	1	Identifies the monitoring policy.
`granularityPeriods`	Integer	0..N	The period between generation of two successive analyses.
`analyses`	STRUCT	0..N	Identifies the analysis (with its associated parameters and methods) conducted on indicated measurement data (see notes 1, 2, and 3).
NOTE 1: In the present table, the analysis and granularityPeriod attributes have the same multiplicity and are ordered to have a 1-1 mapping to specify how often the analysis is performed. NOTE 2: The actual analysis of data and derivation of actions is out of scope. NOTE 3: The detailed definition of analyses is out of scope.			

6.2.4 Type: AlertsMonitoringPolicy

This type indicates to the SMMF the alerts that it may generate based on the analysis of the collected data.

Table 6.2.4-1: Attributes of AlertsMonitoringPolicy

Attribute name	Data type	Cardinality	Description
policyId	String	1	Identifies the monitoring policy.
securityAlerts	STRUCT	0..N	The security alert generated based on analysis.
NOTE: The securityAlerts attribute is described in clause 6.5.2.			

6.2.5 Type: ControlPolicy

This type indicates to the SMMF the security directives that it may send to a given MEC entity due to certain alerts.

Table 6.2.5-1: Attributes of ControlPolicy

Attribute name	Data type	Cardinality	Description
policyId	String	1	Identifies the control policy.
securityDirectives	STRUCT	0..N	The security directive that is issued based on a security alert.
NOTE: The securityDirectives attribute is described in clause 6.4.2.			

6.3 Profile data types

6.3.1 Introduction

A profile data type specifies the capabilities of a MEC entity with respect to SMM. A profile is determined for each MEC entity based upon its implementation and configuration.

6.3.2 Type: MonitoringProfile

This type represents the specific operational measurements that a MEC entity can produce.

Table 6.3.2-1: Attributes of MonitoringProfile

Attribute name	Data type	Cardinality	Description
profileId	String	1	Identifies the profile.
measurementParameters	STRUCT	0..N	Identifies the measurements to collect and corresponding periodicities, as well as events to monitor for.
NOTE 1: The detailed definition of measurements is out of scope. NOTE 2: The measurementParameters attribute is described in clause 6.6.2.			

6.3.3 Type: DirectiveProfile

This type represents the security directives (from the SMMF) that the MEC entity may respond to.

Table 6.3.3-1: Attributes of DirectiveProfile

Attribute name	Data type	Cardinality	Description
profileId	String	1	Identifies the profile.
securityDirectives	STRUCT	0..N	The security directive(s) that the MEC entity may respond to.
NOTE: The securityDirectives attribute is described in clause 6.4.2.			

6.4 Directive data types

6.4.1 Introduction

A directive data type specifies the action to be taken by a MEC entity. The security alert that triggers this action is determined by the SMMF. The detailed definition of actions is out of scope. An example of a potential value for the action attribute in table 6.4.2-1 is an indicator to terminate a MEC application instance in the scenario where a security alert indicates that the MEC application instance is potentially compromised.

6.4.2 Type: SecurityDirective

Table 6.4.2-1: Attributes of SecurityDirective

Attribute name	Data type	Cardinality	Description
directiveId	String	1	Identifies the directive.
securityAlertId	String	1	The security alert that the directive addresses (see note).
actions	String	1..N	The action(s) to take due to the security alert.
timeStamp	String	1	Specifies the point in time when the directive was issued in response to the security alert.
NOTE: The securityAlertId corresponds to the alertId attribute of an associated SecurityAlert in clause 6.5.2.			

6.5 Alert data types

6.5.1 Introduction

Alerts are notifications generated when data analysis triggers specific conditions. Alerts are sent from the SMMF to OSS.

6.5.2 Type: SecurityAlert

Table 6.5.2-1: Attributes of SecurityAlert

Attribute name	Data type	Cardinality	Description
alertId	String	1	Identifies the alert.
timeStamp	String	1	Specifies the point in time in which the alert occurred.
measuredEntities	String	1..N	Identifies the affected MEC entity.

6.6 Measurement data type

6.6.1 Introduction

The MeasurementParameter type in clause 6.6.2 specifies the measurements and events to collect, as well as the periodicity.

6.6.2 Type: MeasurementParameter

Table 6.6.2-1: Attributes of MeasurementParameters

Attribute name	Data type	Cardinality	Description
measurements	String	0..N	The measurement the MEC entity takes over an indicated interval (see notes 1 and 2).
granularityPeriods	Integer	0..N	The period between generation of two successive measurements.
events	String	0..N	The event the MEC entity may observe.
NOTE 1: In the present table, the measurement and granularityPeriod attributes have the same multiplicity and are ordered to have a 1-1 mapping to specify how often the measurement is performed. NOTE 2: The detailed definition of measurements is out of scope.			

7 Security-related Data Examples (informative)

This clause provides a non-exhaustive list of examples of security-related data that may be collected by the SMMF from various MEC entities for the purpose of security monitoring.

Table 7-1: Security-related Data Examples

Data	Possible source MEC entities	Description	Remarks
MEC application lifecycle logs	MEO	Logs of application lifecycle events (e.g. onboarding, instantiation, termination)	Monitor for anomalous MEC application lifecycle events
Cryptographic material management logs	MEP, MEC apps (if applicable), AA Server (out of scope)	Logs of events involving creation, import, export, or deletion of cryptographic keys and certificates	Monitor for manipulation of trusted credentials
Resource utilization	VIM	CPU, memory, storage, and network telemetry	Monitor for potential Denial-of-service
API requests and responses	MEO, MEP, MEPM, MEC Apps	Logs of HTTP requests and responses exchanged via MEC interfaces (e.g. Mp1)	Monitor for API requests and responses for potentially anomalous activity
Network control data	MEP, MEPM	Traffic and DNS rules/configurations	Monitor for unauthorized traffic redirection or misrouting
Security event logs	API Gateway for client applications (AGW), MEC apps	Logs of security-related event types of a MEC entity (e.g. user password changes, failed logons, etc.)	Monitor for unauthorized access attempts, suspicious changes to sensitive attributes
Telemetry data	MEPM, VIM	Operational data including statistics, events, records, and config data	Monitor operational data for potential anomalies or misconfiguration

History

Version	Date	Status
V4.1.1	February 2026	Publication