

Draft Recommendation Y.MOC-Reqts

Requirements for support of machine oriented communication applications in the NGN environment

Summary

This Recommendation provides an overview of machine oriented communication (MOC) applications, including a description of the MOC ecosystem, key supporting features and some relevant use cases. It also analyzes service requirements of MOC applications, specifies extended or new NGN capability requirements and MOC device domain capability requirements based on the service requirements, and provides a reference framework for MOC capabilities.

Keywords

machine oriented communication (MOC), MOC devices, MOC gateway, NGN, MOC applications, NGN capabilities, service requirements

Table of Contents

1	SCOPE	1
2	REFERENCES	1
3	DEFINITIONS	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in this Recommendation	2
4	ABBREVIATIONS	4
5	CONVENTIONS	5
6	INTRODUCTION	5
6.1	Network overview	5
6.2	Types of machine oriented communications	7
6.3	MOC ecosystem	9
7	KEY FEATURES FOR SUPPORT OF MOC APPLICATIONS	12
8	SERVICE REQUIREMENTS OF MOC APPLICATIONS	13
8.1	Mobility levels	13
8.2	Time controlled network communications	14
8.3	Resource usage	14
8.4	Heterogeneous network inter-working	14
8.5	Network access of legacy MOC devices	15
8.6	Application collaboration	15
8.7	Load balancing and robustness	15
8.8	Accounting and Charging	15
8.9	Management	16
8.10	Addressing and identification	17
8.11	Location-based support	18
8.12	Group-based support	18
8.13	Quality of Service	19

8.14	Security	20
8.15	Interaction with multiple applications	21
8.16	Communication with sleeping device	21
9	NGN DOMAIN CAPABILITY REQUIREMENTS FOR SUPPORT OF MOC APPLICATIONS	21
9.1	Requirements for extensions or additions to NGN capabilities	21
9.2	Requirements supported by existing NGN capabilities	24
10	MOC DEVICE DOMAIN CAPABILITY REQUIREMENTS FOR SUPPORT OF MOC APPLICATIONS	25
10.1	Application Enablement	25
10.2	Mobility	25
10.3	Communication	26
10.4	QoS	26
10.5	Remote management	26
10.6	Addressing	27
10.7	Security	27
10.8	MOC device identifier management	27
10.9	Charging	28
11	REFERENCE FRAMEWORK FOR MOC CAPABILITIES	28
11.1	High level view	28
11.2	MOC capabilities in the NGN domain	29
11.3	MOC capabilities in MOC device domain	32
11.4	MOC Service interfaces	34
APPENDIX I		36
I.1	e-Health	36
I.2	Tsunami warning service	38
I.3	Motorcade Management	39
I.4	Oil well monitor	40
I.5	Patrol and surveillance	40

I.6 Smart metering	41
I.7 Video surveillance	42
I.8 Smart home	43
I.9 Integration with Internet services	44
APPENDIX II	47
BIBLIOGRAPHY	50
ATTACHMENT: LIVING LIST FOR Y.MOC-REQTS	51
Item 1	51
Item 2	52
Item 3	53
Item 4	55

ITU-T draft Recommendation

Requirements for support of machine oriented communication (MOC) applications in the NGN environment

1 Scope

This Recommendation covers extensions and additions to NGN capabilities [ITU-T Y.2201] and MOC device domain capabilities in order to support machine oriented communication (MOC) applications in the NGN environment. Although this Recommendation deals with support of MOC applications in the NGN environment, these capabilities can conceptually be applicable to other networks.

The scope of this Recommendation includes:

- Service overview, description of MOC ecosystem and key supporting features of MOC applications;
- Service requirements to support MOC applications;
- Requirements of extended or new NGN capabilities based on the MOC service requirements;
- Requirements of MOC device domain capabilities (for supporting MOC applications over NGN)
- Reference framework for MOC capabilities.

NOTE - Appendix I provides relevant use cases of MOC applications in the NGN environment.

2 References

The following ITU-T Recommendations and other references contain provisions, which through the references in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.2221] ITU-T Recommendation Y.2221 (2010), *Requirements for support of Ubiquitous Sensor Network (USN) applications and services in the NGN environment*

[ITU-T Y.2012] ITU-T Recommendation Y.2012 (2010), *Functional requirements and architecture of the NGN*

[ITU-T Y.2201] ITU-T Recommendation Y.2201 (2009), *Requirements and capabilities for ITU-T NGN*

[ITU-T Q.1706] ITU-T Recommendation Q.1706/Y.2801 (2006), *Mobility management requirements for NGN*.

[ITU-T Y.2111] ITU-T Recommendation Y.2111 (2008), *Resource and admission control functions in next generation networks*.

[ITU-T Y.2233] ITU-T Recommendation Y.2233 (2008), *Requirements and framework allowing accounting and charging capabilities in NGN*.

[ITU-T Y.2701] ITU-T Recommendation Y.2701 (2007), *Security requirements for NGN release 1*.

[ITU-T Y.2720] ITU-T Recommendation Y.2720 (2009), *NGN identity management framework*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 network mobility [ITU-T Q.1703]: The ability of a network, where a set of fixed or mobile nodes are networked to each other, to change, as a unit, its point of attachment to the corresponding network upon the network's movement itself.

3.1.2 Open Service Environment capabilities [ITU-T Y.2234]: Abilities provided by an open service environment to enable enhanced and flexible service creation and provisioning based on the use of standards interfaces.

3.1.3 NGN Service Integration and Delivery Environment (NGN-SIDE) [ITU-T Y.2240]: An open environment in NGN integrating resources from different domains and delivering integrated services to applications over NGN.

NOTE - these domains include, but are not limited to, Telecommunication domain (e.g. Fixed and Mobile Networks), Internet domain, Broadcasting domain and Content Provider domain.

3.1.4 sensor [ITU-T Y.2221]: An electronic device that senses a physical condition or chemical compound and delivers an electronic signal proportional to the observed characteristic.

3.1.5 gateway [ITU-T Y.2091]: A unit which interconnects different networks and performs the necessary translation between the protocols used in these networks.

Editor's note: inclusion of the definition for UICC should be considered (according to device management requirements in clause 8).

3.2 Terms defined in this Recommendation

Editor's note: These definitions should be reviewed against the terminology already defined in the MOC area in other ITU-T Recommendations (e.g. Y.2221) or by other SDOs (e.g. ETSI M2M, 3GPP etc.) and see if adoption or harmonization with some already defined terms could be made (with or without possible amendments).

Editor's note: it is for consideration to make the various definitions NGN-independent (e.g. mentioning the relationship with NGN (in scope of this recommendation) as NOTES to the definitions or via a convention clause).

This Recommendation defines or uses the following terms:

3.2.1 MOC: A form of data communication between two or more entities in which at least one entity does not necessarily require human interaction or intervention in the process of communication.

3.2.2 MOC device: A device with limited or no human intervention involved in the support of MOC applications.

NOTE - In the NGN environment, a MOC device connects with NGN directly or indirectly through a MOC gateway. A MOC device can be a limited-capability device, e.g., a sensor an actuator, or a high-capability device, e.g., a camera or a smart phone.

Editor's note: the followings are considerations from drafting on which contributions are invited to classify meaningfully the different types of MOC devices: "The following entities can be a MOC device:

- ***Non-human-driven device** (e.g., sensor, surveillance camera, meter, actuator with remote control)*
- ***Thing-associated communication entity** (e.g., RFID/printed-ID and reader)*
- ***Logical communication entity** (e.g., movie, segments of content)*
- ***gateways and proxies representing multiple entities above** (e.g., GW for protocol conversion, tentative data storage, and a proxy representing devices in a car)*
- ***Human-driven communication entity** (e.g., black phone, mobile phone, communication software in PC, web browser, networked TV)"*

3.2.3 MOC application: An application that runs application logic and uses MOC capabilities accessible via standard interfaces.

NOTE - In the NGN environment, a MOC application communicates with MOC devices and/or MOC gateways through NGN, for e.g. instruction delivery and data collection purposes.

3.2.4 MOC gateway: A gateway which interconnects MOC local networks and the NGN.

NOTE - A MOC gateway acts as a proxy or data aggregator to ensure inter-working and interconnection of MOC devices with the NGN.

3.2.5 MOC group: A list of MOC devices and/or gateways grouped according to one or multiple criteria.

NOTE - Criteria may include MOC application subscriber, MOC device manufacturer, MOC application, location.

3.2.6 actuator: A device performing physical actions caused by an input signal.

NOTE - As examples, an actuator might act on the flow of a gas or liquid, on the electricity distribution, through a mechanical operation. Dimmers and relays are examples of actuators. The

decision to activate the actuator may come from a MOC application, human or MOC device/gateway.

3.2.7 MOC end user: An end user of MOC applications.

NOTE - This end user may be a system (e.g. MOC application server, other network equipment, other applications, MOC device, MOC gateway), or a human (e.g. NGN end user).

3.2.8 MOC local network: A network which provides connectivity between MOC devices without the intermediation of MOC gateway, and between MOC devices and MOC gateways.

NOTE - A MOC local network may provide IP based and/or non-IP based connectivity.

3.2.9 MOC capabilities: a set of functions for the support and management of MOC applications, which can be shared by different MOC applications, and are accessed through a set of standard interfaces.

NOTE - MOC capabilities provide standard interfaces for MOC applications to MOC devices and/or gateways for data collection, management and operation. MOC capabilities reuse or interact with NGN capabilities [ITU-T Y.2201] [ITU-T Y.2240], IT capabilities or Internet capabilities to provide MOC applications.

3.2.10 meter

A device that measures and optionally records the quantity, degree, or rate of something, especially the amount of electricity, gas, or water used.

NOTE: A meter is responsible for measuring the total amount of something consumed in a period.

4 Abbreviations

This draft defines or uses the following terms:

ACI	Application to Capability Interface
ANI	Application to Network Interface
GPS	Global Positioning System
GNSS	Global Navigation Satellite Systems
IP	Internet Protocol
IT	Information Technology
MOC	Machine Oriented Communication
NGN	Next Generation Network
NNI	Network to Network Interface
OSE	Open Service Environment
QoS	Quality of Service
SIDE	Service Integration and Delivery Environment
SNS	Social Network Services

UICC Universal Integrated Circuit Card
UNI User to Network Interface
USN Ubiquitous Sensor Network

5 Conventions

In this Recommendation:

The keywords “is required to” indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords “is recommended” indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords “can optionally” and “may” indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor’s implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Introduction

6.1 Network overview

Machine oriented communications (MOC) refer to communications between two or more entities that need limited or even no direct human intervention.

Machine-oriented communications include communications with remote devices for monitoring, management and other functions. MOC applications intend to automate decision and communication processes.

Editor’s note: the following text (in italic) should be considered for deletion after finalization of clause 6.2.

“There are several phases for MOC applications execution in NGN environment: data collection data transportation, data analysis, information delivery and information reception.

- Data collection: MOC devices detect, measure and record data (e.g. data related to a physical properties, multimedia data, physical objects status etc.) and converts to data signal. When a MOC device meets a trigger threshold or receives an instruction, it requests the NGN to transfer the data to the MOC application.*
- Data transportation: NGN establishes a data path between MOC devices and MOC applications, and transfers data from MOC devices to MOC applications.*
- Data analysis: the MOC application analyzes data after receiving data from MOC devices to obtain different kinds of information.*
- Information delivery: the MOC application executes service logic and decides how to publish the information to end users (including MOC devices and humans) or other applications. Information delivery can be “active” meaning that the MOC application pushes information to the end user automatically. The MOC application also supports pushing the information based on demand from end user (“passive” information delivery”).*
- Information reception: the receiving party can be an end user or another MOC application (they may execute other actions after having received the information).*

NOTE: not all of the above phases are necessary in all MOC applications. For example, a NGN end user can send a request to the MOC application to turn on the klaxon when he/she wants to find out his/her car in a large parking, and the control centre of vehicles will turn on the switch for the user after receiving the request. In this example, data collection and data transportation from the MOC device (vehicle) to the MOC application is not executed.”

Figure 6-1 shows a network overview for the support of MOC applications in the NGN environment.

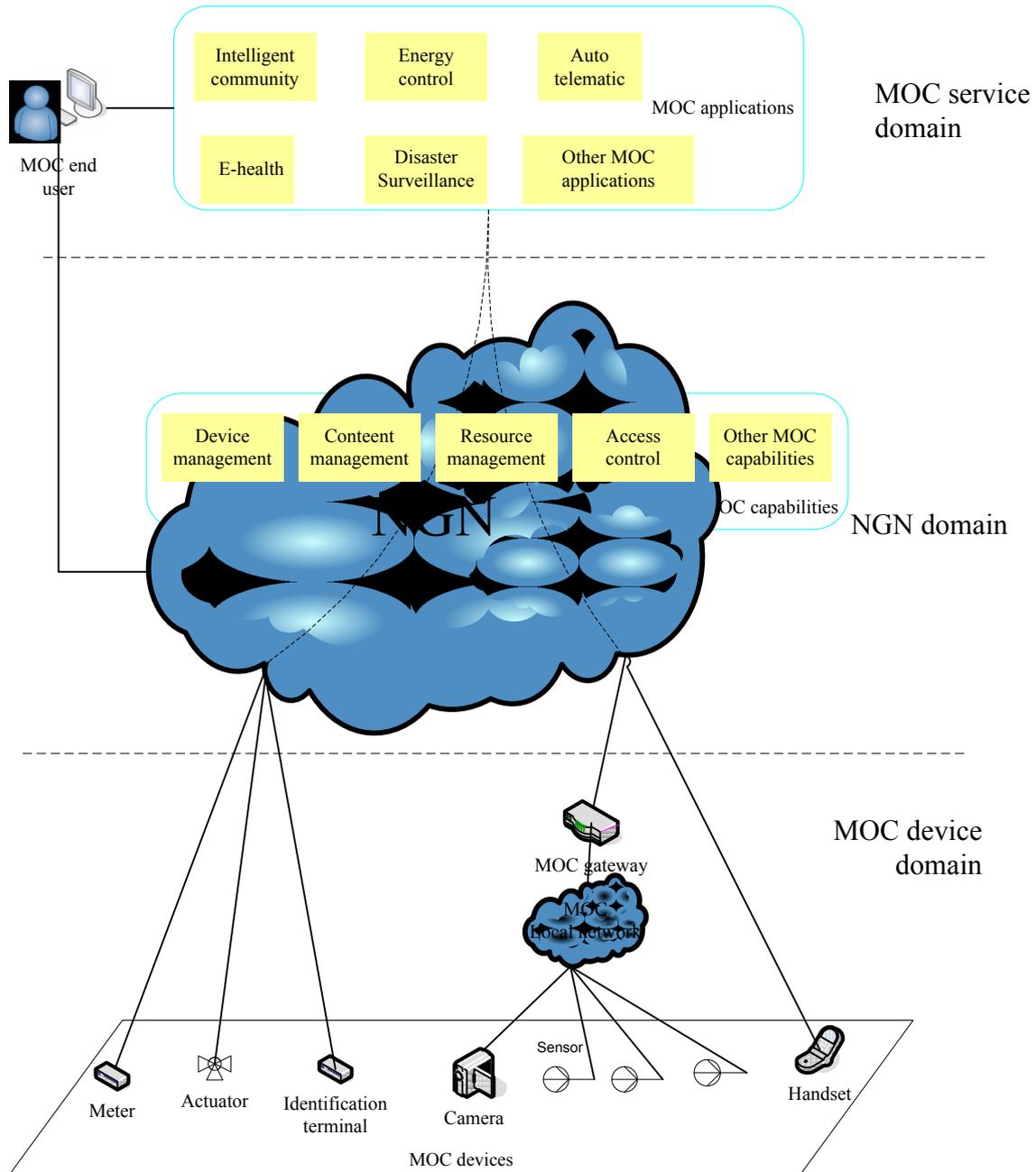


Figure 6.1 MOC network overview in the NGN environment

Editor's note: It should be considered if "MOC application manager" is another relevant entity in the picture. The "MOC end user" entity position should be confirmed.

Editor's note: it is to be clarified which distinct types of MOC devices (possibly, including their definitions) are meaningful for distinction in figure 6.1 (e.g. meter, identification terminal, handset): their distinction should be meaningful in terms of relevance for the recommendation (MOC requirements, NGN capabilities). See also details in the editor's note for the "MOC device" definition.

Editor's note: Terms in figure 6.1 should be aligned with definitions of MOC device.

Editor's note: it should be considered the possibility to have a generic network independent picture and a specific picture with NGN as the network.

MOC device domain includes MOC devices and MOC gateways. MOC devices include various types of devices as shown in figure 6.1.

MOC devices may access to the NGN directly or via a MOC local network and MOC gateways attached to it. MOC devices or gateways may access the NGN by use of wire-line or wireless connectivity.

MOC devices and MOC gateways may access NGN via multiple access networks (e.g. PLMN and PSTN), for example to ensure reliable communications.

NGN domain not only provides access, data transportation, network control and interconnection (with other networks) functions, but also provides MOC capabilities to support multiple MOC applications.

MOC capabilities reuse or interact with the NGN capabilities, expose functionalities to MOC applications through a set of standard interfaces, provide support to facilitate application development and deployment through hiding of network specificities to MOC applications. MOC capabilities include capabilities for device management, resource management, content management and access control. Details can be found in clause 10.

MOC service domain includes the MOC applications. MOC applications run the application logic and use MOC capabilities accessible via standard interfaces.

6.2 Types of machine oriented communications

MOC cover communications among machines and humans, therefore MOC includes Machine-to-Machine (M-M), Machine-to-Human (M-H) and Human-to-Machine (H-M) communications. The following sub-clauses 6.2.1 to 6.2.3 describe in detail these MOC types.

NOTE – the distinction among M-M, M-H and H-M communications is based upon the following criteria:

- machine or human initiating the communication;
- machine or human receiving the communication.

Editor's note: clauses 6.2.1 to 6.2.3 need detailed review.

6.2.1 Machine-to-Machine communications

"M-M communications" means a MOC device communicating with another MOC device, or **interacting with MOC capabilities** or MOC applications for data collection, device management, device operations and other communication functions with remote equipment and devices to provide many kinds of applications.

In the case of a MOC device interacting with MOC capabilities or MOC applications, the M-M communication based application execution in NGN environment may be divided into the following phases:

- Data collection: the MOC device detects, measures and records data (e.g. data related to a physical properties, multimedia data, physical objects status etc.). When the MOC device meets a trigger threshold or receives an instruction, it requests the NGN to transfer the data to the MOC application.
- Data transportation: the NGN establishes a data path between the MOC device and the MOC capabilities, The MOC application can communicate with the MOC device directly under the authorization of MOC capabilities: the MOC application gets the authorization information from the MOC capabilities which are used for authorization and negotiation of the session key used for secure communication in order to manage the MOC device.
- Data analysis: the MOC application analyzes data received from the MOC device. MOC capabilities can also analyse the data based on rules defined by the MOC end users.
- Service delivery: the MOC application executes the service logic and decides how to publish the information to MOC end users (including MOC devices, humans or other applications). Information delivery can be “active” meaning that the MOC application pushes information to MOC end users automatically. The MOC application also supports pushing the information based on demand from MOC end users (“passive” information delivery”).

MOC capabilities can also interact with other applications, such as Social Network Services (SNS), Blog, Twitter, which can make available the MOC related information according to the requirements from customers or applications.

- Service reception: the customer consumes the information provided by the MOC application or the applications interacting with the MOC capabilities.

There are two cases for a MOC device communicating with another MOC device:

- the first case is when the address of the destination MOC device can be pre-configured in the MOC device initiating the communication for direct communication through the NGN. It is to be noted that the MOC device can also broadcast (or use other ways) its identifier and/or other information to other MOC devices directly.
- the second case is when the MOC device initiating the communication, gets the authorization information from the MOC capabilities for authorization and negotiation of the session key used for secure communication **in order to manage the MOC device.**

6.2.2 Machine-to-Human communications

Editor’s note: text should clarify the role of human.

M-H communications refer to MOC devices communicating with humans. The communications are generally triggered by a MOC device to timely inform about relevant information detected on its own.

The MOC device executes and follows the pre-configured policy, which can be defined by the MOC capabilities or the MOC applications. The MOC device executes the policy and detects data: when the policy execution result meets the conditions defined by the policy, the MOC device executes the logic and triggers the actuator(s) and initiates the communication to the human to report the relevant information.

M-H communications can also provide “push” services to provide information to customers based on customer profiles, location, etc.

6.2.3 Human-to-Machine communications

Human to machine communications are in general initiated by humans with intelligent MOC devices to get relevant information. The intelligent MOC devices can accept or refuse the service requests according to the policy already defined or previously configured by the MOC capabilities.

Human to machine communications have many customer scenarios with usage of mobile or other terminal to detect or get the relevant MOC device information using bar code, RFID, etc.

6.3 MOC ecosystem

Editor’s note: it is needed to describe the relationship between domains in figure 6.1 and the roles in ecosystem.

Editor’s note: the following picture and associated text is an ongoing work. It is expected to identify some key scenarios, each with a limited set of main interacting roles.

Editor’s note: terminology alignment should be considered across the document.

6.3.1 Business roles

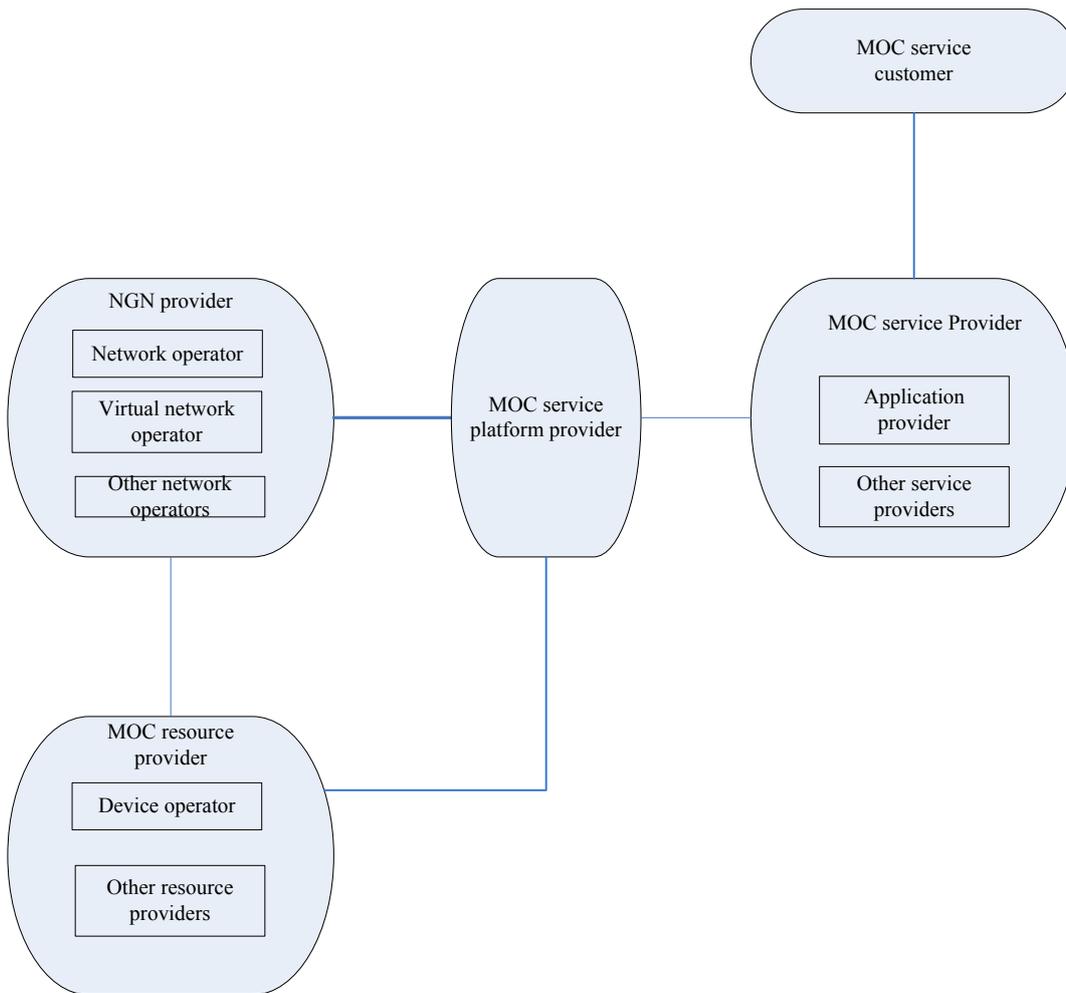


Figure 6.2 Business roles in a MOC ecosystem

Figure 6.2 depicts business roles which are relevant in a MOC ecosystem and their relationships. Five key roles are identified: MOC service customer, NGN provider, MOC resource provider, MOC service platform provider and MOC service provider.

- **NGN provider**

The NGN provider performs the following main functions:

- **Access and integration of resources provided by MOC resource providers;**
- Offering of common NGN capabilities to the MOC platform provider.

For the NGN provider role, the following sub-roles are identified (but not limited to): network operator, virtual network operator and other network operators.

- **Network operator:** the role which provides NGN services with its own NGN infrastructure.
- **Virtual network operator:** the role which provides NGN services but does not have its own NGN infrastructure (for example, it could be leased from a network operator).
- **Other network operators:** the roles which provide services with other network infrastructure.

The NGN provider has business relationship with the MOC service platform provider and the MOC resource providers.

NOTE – An actor playing the role of NGN provider can also play the roles of MOC service platform provider, MOC resource provider and MOC service provider.

- MOC service provider

The MOC service provider utilizes capabilities provided by the MOC service platform provider in order to provide services to the MOC service customer. The following sub-roles are identified (but not limited to):

- Application provider: the role that is responsible for offering application(s) to the MOC service customer.
- Other MOC service providers: the roles that provide other services to the MOC service customer (e.g. providers of e-map, weather forecast).

The MOC service provider has business relationship with the MOC service customer and the MOC service platform provider.

NOTE – An actor playing the role of MOC service provider can also play the role of MOC service platform provider.

- MOC resource provider

The MOC resource provider is responsible for providing raw data or other necessary resources to the NGN provider and the MOC service platform provider according to the service logic.

The following sub-roles are identified (but not limited to):

- MOC device operator: the role that is responsible for the implementation of sensing devices and/or controlling devices and for exchanging information with the NGN provider and the MOC service platform provider. For example, the operator who implements cameras for surveillance can act as MOC device operator.
- Other resource providers: the roles that provide other resources to the MOC service platform provider (e.g. providers of computing, storage resources).

The MOC resource provider has business relationship with the MOC service platform provider and the NGN provider.

NOTE – An actor playing the role of MOC resource provider can also play the role of MOC service provider and the MOC platform provider.

- MOC service platform provider

The MOC service platform provider is responsible for:

- Access to and integration of resources provided by MOC resource providers and the NGN provider.
- Support and control of the service **integration and delivery** functionalities.
- Offering to the MOC service provider of capabilities (including resource exposure) for support of MOC applications.

The MOC service platform provider has business relationship with the MOC resource provider, the MOC service provider and the NGN provider.

NOTE – An actor playing the role of MOC service platform provider can also play the role of MOC service provider and MOC resource provider.

- MOC service customer

The MOC service customer maybe a human or a device. The MOC service customer consumes services offered by the MOC service provider. Organizations or persons such as enterprise, family, individual are examples of MOC service customers.

The MOC service customer has business relationship with both the MOC service provider. The MOC service customer is the subscriber of MOC service.

6.3.2 Actors and related roles in the MOC ecosystem

The following identifies different actors of the MOC ecosystem and the business roles that they can play:

- The “carrier” actor. The "carrier" actor plays the role of NGN provider. Depending on the business scenario, the "carrier" actor can also play the role of MOC service provider, MOC service platform provider and MOC resource provider.
- The “3rd party application provider” actor. The "3rd party application provider" actor plays the role of MOC application provider. Examples of 3rd party application providers include Web based application providers. The “3rd party application provider” actor can also play the role of MOC service platform provider.
- The "3rd party resource provider" actor. The "3rd party resource provider" actor plays the role of MOC resource provider. Examples of 3rd party resource providers include storage providers, end users. The "3rd party resource provider" actor can also play the roles of MOC service platform provider and MOC service provider.

7 Key features for support of MOC applications

Editor’s note: it is needed an editorial review of the whole clause and reordering (for devices, for applications etc.).

MOC applications and devices do not all have the same characteristics. The key features for support of MOC applications include but are not limited to the following ones:

1) Group functionalities

In many use cases, groups of MOC devices are deployed for special services. Usually, the MOC devices of a specific group have same technology, functions, performance, policies.

2) Different mobility levels

Many MOC devices will be moving everywhere. Some of devices will not move. Some of devices will be moving only within a certain area.

3) Different security levels

MOC devices are not operated manually and remote management is required. This increases the security threat level, such as physical tampering, hacking, unauthorized monitoring and so on. So MOC devices should provide adequate security policy to detect or resist the attacks.

4) Various capabilities of MOC devices

There are massive devices for different usage. Some MOC devices have low performance and limited functionality. This type of MOC devices usually has low processor or small memory which could not provide some security features, encryption data, for example.

Some MOC devices have high capabilities which can include bilateral authentication and authorization with network or MOC applications.

5) Remote management

Because massively deployed MOC devices cover large areas, exist for a long time and may be moving, it is difficult for operators or subscribers to physically manage all devices.

Remote management functionality of MOC devices is required, for example updating the firmware to correct faults.

6) Heterogeneity of devices

A MOC application may use more than one type of devices. These types of devices could use different physical layers or be operated differently in IP-based or non-IP based networks.

7) Different data communication types

Most of MOC applications depend on data communications. The types of MOC data communications are much different from human communications.

According to packet size, data communications can be classified into large or small packet communications. According to data transmission period, data communications can be classified into more or less frequent communications.

According to the initiating party of a data communication, data communications can be classified into MOC device terminated or MOC device originated.

8) Common MOC capabilities

There are many types of MOC devices and applications. Some common MOC capabilities, such as device management, device monitoring, application management, are needed in order to deploy different types of MOC devices and MOC applications in flexible way.

8 Service requirements of MOC applications

Editor's note: Requirements for the MOC device domain (MOC devices, MOC gateway, MOC local network) in this clause should be moved to clause 10.

Editor's note: all text (initial descriptions and requirements) in all clauses 8.X should be written in terms of MOC service requirements (related requirements of the network are in clause 9).

Editor's note: it is still an open point if the requirements in the draft Y.SCN should be considered to enhance the requirements of Y.MOC.

8.1 Mobility levels

Editor's note: the requirement needs further explanation concerning the implications of low mobility management. It is also required to detail further the types of mobility (device, gateway).

Different types of MOC applications may require different levels of MOC device and/or gateway mobility. This includes no mobility for devices/gateways that do not move, infrequent mobility for devices/gateways that move infrequently (e.g., one or two times per month), or low geographical mobility for devices/gateways that move only within a certain region (e.g., one cell). Requirements of mobility levels are as follows:

- 1) MOC applications are required to be supported with optimized mobility management according to the required levels of mobility.

Editor's note: the detailed requirements for mobility of MOC devices/gateways should be developed.

8.2 Time controlled network communications

In order to minimize cost and optimize the network efficiency, MOC devices or MOC gateway can cache locally the collected data and transmit them to the network during the time slots allowed or pre-configured by the network operator. The requirements for time controlled network communications are as follows:

- 1) MOC applications require support of time control for MOC device communications with the network based on service criteria (e.g. daily network traffic load, MOC device location).
- 2) MOC applications require support of setting and modification for MOC end users' (granted/forbidden) network communication access time schedules and durations.
- 3) MOC applications require that (granted/forbidden) network communication access time schedules and durations are communicated to the MOC devices.

8.3 Resource usage

MOC applications are expected to involve low resource usage in the case where MOC devices are expected to send or receive data infrequently (i.e. with a long time period between two data transmissions). To improve network efficiency and decrease the MOC application operational costs and MOC device energy consumption, both resources of MOC devices and NGN need to be optimized.

MOC applications requirements for optimized resource usage are as follows:

- 1) MOC applications are required to be supported in optimized way, including the case of infrequent data transmissions.
- 2) MOC devices are required to be turned offline (i.e. no active connection) when no data transmission is required.

8.4 Heterogeneous network inter-working

Editor's note: the requirement needs further explanation about the need for heterogeneous network inter-working. Existing networks should be positioned in the picture above and the scenario clarified in the text below.

MOC applications should be able to inter-work with existing networks to provide more flexible and ubiquitous service experience since there have been deployed various service systems, e.g., Cable TV network, meteorology network, public safety network, banking network, enterprise network, e-Health system, etc. The inter-work may include both transport layer and service layer. For transport layer, it should support mechanism such as trans-code, etc.; for service layer, it should support service adaptation, such as service data format adaptation, service interaction control, security management, etc.

- 1) MOC applications require support of inter-working between heterogeneous networks.

8.5 Network access of legacy MOC devices

Editor's note: the requirement needs further explanation about the need for legacy MOC devices access. Legacy MOC devices should be positioned in the picture above (is it a definition required or other terminology should be used?).

Editor's note: it should be considered if this requirement is only for network access or more generally for MOC application operation.

Since a lot of legacy MOC devices and gateways (e.g., devices with proprietary standards for inter-working with network entities) have already been deployed, MOC applications should be able to support network access of such kind of devices.

1) MOC applications require support of network access by legacy MOC devices.

8.6 Application collaboration

Editor's note: the requirement needs further explanation about the need for application collaboration and the parties involved. It is also required further elaboration on the scenario(s) (e.g. MOC service provider, other 3rd party service providers, NGN provider).

For MOC applications, there might be multiple service providers involved in the MOC application provisioning which can collaborate between each other. For example, when MOC devices transmit data to network, the network may support routing data to multiple target service providers and network may need support selecting and correlating these services intelligently.

One application scenario example is that NGN should support routing diagnosis data from MOC devices to multiple hospitals so that different hospitals may receive different types of data and they can diagnose patient jointly.

1) MOC applications require support of application collaboration between service providers.

8.7 Load balancing and robustness

Editor's note: the requirement needs further explanation about the need for load balance and robustness, including which is the requirement for MOC applications.

MOC devices may be distributed variously in territory, and the density of MOC devices in a certain area may be high or low. This may cause system imbalance accordingly for both signalling and data traffic. In order to support load balancing and high availability, the requirements are as follows:

1) MOC applications require load balancing and robustness support for both signalling and data traffic.

8.8 Accounting and Charging

Different charging and accounting requirements might be addressed depending on the scenarios of MOC applications. For example, there are MOC applications with frequency data transmission and small amounts of data, in this case charging and accounting could base on the number of communication times. Some other MOC applications may rarely connect to NGN but generate large amounts of data for each connection, in this case, charging and accounting could base on the amount of data. In other cases charging and accounting could base on the duration of communication.

As many MOC applications may be used in multiple devices for one user, if the operator or 3rd party service provider charges each device, there would be many charging data records (CDR) which will impose heavy load to some entities, e.g. the charging entity. In these scenarios,

group-based accounting and charging instead of per device accounting and charging may be more appropriate.

MOC applications have the following requirements:

- 1) MOC applications is required to support different charging and accounting methods, such as charging base on the duration of communication, communication times, amount of data transmission etc.
- 2) MOC applications require support of unified charging for customers;
- 3) MOC applications require support of accounting & charging based on groupings.

8.9 Management

Editor's note: text in this clause needs to be fully reviewed and restructured in terms of requirements of MOC applications.

8.9.1 Device management

Editor's note: a definition of UICC is needed. The relationship of UICC and MOC device should be clarified in order to understand the usage of UICC in this clause.

MOC devices cover a large area, exist for a long time and could be moving. It's impossible for operators or subscribers to manage these devices physically by humans. Thus, MOC device/gateway should be managed and monitor remotely (for example, updating the firmware to correct faults).

A MOC device (or UICC) may be used illegally (e.g. when the MOC device or UICC is stolen without awareness). Thus, the change of the state of the MOC device should be accessible by the MOC application

When MOC device/gateway provides service logic, the MOC device/gateway is a service enabler device and provides added value for both the customer and the service. MOC device/gateway is required to be managed in terms of both network and service management.

For a large proportion of MOC devices, they usually have low capabilities and some general device management protocols are not applicable to them.

The requirements of MOC device management are as follows:

- 1) MOC applications are required to support mechanisms for managing gateways acting as traffic aggregators (a gateway aggregates traffic and acts as a channel).
- 2) MOC applications are required to monitor the state of MOC devices and gateways for various aspects, including:
 - a) Abnormal behaviour of MOC device/gateway, such as acting service not aligned with the subscribed feature;
 - b) the association between the MOC device/gateway and the UICC;
 - c) the attachment information of MOC devices/gateways, such as attachment location;
 - d) the connectivity of MOC devices/gateways
- 3) MOC applications are required to support mechanisms to perform simple and scalable pre-provisioning of MOC devices/gateways, enabling and disabling features, report errors from the device, query about their status.

4) MOC applications are required to support mechanisms to perform software upgrades (e.g. provisioning of new service logic and/or bug fixes to be loaded on the devices/gateway, including applications and system software).

5) MOC applications are required to manage low capability MOC devices using light-weight mechanisms.

8.9.2 Service profile management

Data may be utilized by different MOC applications and are manipulated as different service data based on the different MOC application needs.

The MOC service profile is a way to support the various characteristics and demands of data usage. The service profile of a specific MOC application is composed by a set of information specific to that MOC application. It may include, but it is not limited to, MOC application identifier, data types, MOC service provider and **location information**.

MOC applications have the following requirements:

- 1) MOC applications are recommended to use standard MOC service profiles for their registration and discovery.
- 2) MOC applications are required to support mechanisms to perform service profile updates.

8.9.3 Device profile management

The MOC device profile is a set of information related to the MOC device and/or the MOC gateway. As there are various types of MOC devices and MOC gateways, the device profiles would be helpful to manage a large number of heterogeneous devices, gateways and local area networks. The information of MOC device profiles may include MOC device identifier, device type, device capabilities and the location of the MOC device.

MOC applications have the following requirements:

- 1) MOC applications are recommended to use standard MOC device profiles containing the MOC device and/or the MOC gateway related information.

8.10 Addressing and identification

Editor's note: the requirements need further elaboration.

There are two types of connection methods between MOC devices and MOC applications. MOC devices may connect to MOC applications directly or via MOC gateways based on IP connectivity. Different MOC devices may communicate to different MOC applications via a single MOC gateway or via multiple gateways. NOTE - the second scenario allows to decrease each MOC gateway's load and to increase the network access reliability.

MOC devices may support public or private IP addresses, and may also support non-IP addresses when they connect to the NGN via MOC gateways. In an IP based network, MOC application servers/devices which are using public IP addresses should be able to communicate with other MOC devices which are using private IP addresses.

The requirements of addressing and identification are as follows:

- 1) MOC applications require support of addressing mechanisms so that MOC applications are able to communicate with MOC devices behind a MOC gateway.
- 2) MOC applications require support of unique identification of MOC devices.

8.11 Location-based support

The MOC device/gateway' location information may include GNSS (e.g. GPS) latitude or longitude data, CellID and so on. Device management, device discovery, context awareness may be supported with usage of location information.

- 1) Location data may be collected by the MOC applications from the MOC device/gateway or network, using the following possible methods: The MOC device sends the GNSS geographical information collected by itself to the MOC application via a data transmission channel.
- 2) If the GNSS geographical information cannot be provided by the MOC device/gateway, the MOC application may get location information from the network.

MOC applications have the following requirements:

Editor's note: it should be clarified if (and only if) all following requirements apply to MOC applications.

- 1) MOC applications are required to be aware of the location of the MOC devices. For example, based on the location information of MOC devices, the MOC application could initiate a service trigger to upgrade the firmware on the MOC devices within a certain area by broadcast/multicast method.
- 2) In some application scenarios, it is required to maintain and manage location information both of single MOC device and a group of MOC devices behind a MOC gateway.
- 3) In some application scenarios, it is required to maintain and manage different types of location information.

8.12 Group-based support

MOC groups may be used in many MOC applications. For example, a vehicle company owner could manage the company vehicles in groups, e.g. track the locations of all the vehicles in the group, and send notification messages to all the vehicles in the group. An electricity company could collect the metering data of all the MOC devices in a certain area at a certain time. A consumer could query the different meters at his home when he is on a business trip.

Different MOC applications may have different MOC groups and these MOC groups should be uniquely identified in NGN.

MOC applications may have static MOC groups which are pre-configured, for example the consumer could pre-configure his MOC devices (e.g. metering equipment) installed at his home into a MOC group. MOC applications may also have dynamic groups which are grouped according to some on-demand criteria, for example a vehicle company owner may request to communicate with all the vehicles in a certain area when needed.

When MOC applications need to send/receive information to/from all members in the group, the MOC applications should be allowed to send the request in a single command, i.e. using group identifier. The MOC applications could request to send/receive information to/from all members in a group or a single member in a group.

The MOC devices inside a group may directly connect to NGN or indirectly connect to NGN.

MOC applications should be able to request to charge based on the group either for on-line charging or for off-line charging.

It should be able to define the group based QoS policy according to the business contract between the MOC service provider and the user, e.g. based on the QoS policy parameters such as priority and packet error ratio.

It should be able to define the group based traffic parameters according to the business contract between the MOC service provider and the user, e.g. maximum bandwidth, peak data rate.

MOC applications should be able to manage the MOC groups, e.g. to create and remove a MOC group, to add, remove and list the members of a MOC group.

The requirements for group-based support are the following:

- 1) MOC applications require support of static and dynamic MOC groups.
- 2) MOC applications require unique identification of MOC groups.
- 3) MOC applications require support of data transmission to/from one or all members in a MOC group using group identifier.
- 4) MOC applications require support of group based QoS policy.
- 5) MOC applications require support of group based traffic parameters.
- 6) MOC applications require support of group-based charging either for on-line charging or for off-line charging.
- 7) MOC applications require support of MOC group management, including display/create/modify/delete of MOC groups and associated attributes, display/add/modify/delete of MOC group members.
- 8) MOC applications are recommended to be able to send data per MOC group, and appoint data prioritization according to member's data prioritization in MOC group.

8.13 Quality of Service

Editor's note: the requirement needs further explanation about the need for QoS management, and the requirements may also need further elaboration.

8.13.1 Application traffic control

The application traffic is not only generated by the MOC devices, but also generated by the MOC applications. From the viewpoint of applications, the QoS of MOC applications may be impacted in case of high application traffic.

From the viewpoint of NGN, the QoS of MOC applications may be improved in case that the high application traffic is managed well. The following requirements are placed on both network and application/service provider's resources:

- 1) MOC applications is required to manage the transaction volume from/to applications and services.
- 2) MOC applications is required that an access concentration into a single resource is avoided.

8.13.2 Data prioritization

The MOC mission-critical applications and services should be carefully managed. For example, emergency notification of a fire incident must be delivered in a timely and reliable way to the

appropriate national disaster monitoring systems. The emergency data are carried over the NGN to provide alarm notification.

MOC applications have the following requirements:

- 1) MOC applications are recommended to be able to set the prioritization of certain types of data. (within a single application or among different applications)
- 2) MOC applications are recommended to be able to manage different data according to the data prioritization.
- 3) MOC applications are recommended to be able to appoint data prioritization by MOC devices or MOC gateways according to Service Level Agreement

8.14 Security

8.14.1 Authentication and Authorization

NGN providers and MOC service providers must verify the identification of MOC end users to access MOC applications.

For MOC devices connected via a MOC gateway, the authentication of MOC devices may be performed directly by the MOC application or via the MOC gateway authentication.

Requirements of authentication and authorization are as follows:

- 1) MOC applications are required to support identification, authentication and authorization of MOC end users to access different types of data according to the related security level.
- 2) MOC applications are recommended to support a mechanism for identification, authentication and authorization of MOC devices which are in a MOC local network.

8.14.2 Security of data

In general, MOC applications require strong security, due to very sensitive data. It has to be considered that MOC devices cannot provide all security features because they may have system limitations. For example, sensed data carried over the network may not be sufficiently protected from security view point (e.g. encrypted as required).

MOC applications have the following requirements:

- 1) MOC applications are required to provide security for the connectivity between MOC applications and MOC devices even when some of the MOC devices are connected via a roaming operator.
- 2) MOC applications are required to support verification of the integrity and confidentiality of the data exchanged
- 3) MOC applications are **recommended** to provide mechanisms of data encryption in order to support also MOC devices with limited capabilities.

8.14.3 Security of MOC device access

All data produced by MOC devices shall be unknown to unauthorized entities. For example, private or sensitive data of a MOC device should not be sent to an unauthenticated NGN end user if the NGN end user initiates a communication with that MOC device **directly**.

Due to the limited capabilities of the MOC devices with no support of authentication and authorization functionalities:

1) Before the resource of MOC devices can be used by end-users or applications, it is required to be able to check the identification, authentication and authorization of end-users and MOC applications.

2) The MOC devices can optionally identify and authenticate MOC applications, other MOC devices, or other MOC end users.

8.15 Interaction with multiple applications

In some application scenarios, a single MOC device may require to communicate with different MOC applications simultaneously. For example, when a traffic accident happens, the damaged vehicle may be required to provide information to both the health service centre and the department of traffic control.

MOC applications have the following requirements:

1) MOC applications are required to allow collection/delivery of MOC devices/gateways information from/to multiple MOC applications.

8.16 Communication with sleeping device

In case of offline status for a given period of time, some MOC devices are recommended to enter/stay in sleeping mode in order to:

- save power supply, especially for devices using a battery
- save network resources, especially for devices with wireless network access

NOTE - Sleeping mode is an energy-saving mode. It normally refers to a MOC device in a situation when traffic is not generated for a period of time, device sessions and related traffic channel are released to save resources, and all unnecessary components are shut down. According to certain criteria, a MOC device in offline status can enter in sleeping mode.

MOC applications have the following requirements:

- 1) MOC applications should be able to send an instruction to a sleeping MOC device to wake it up.
- 2) MOC applications are required to support network-initiated communications towards a sleeping MOC device.

9 NGN domain capability requirements for support of MOC applications

Editor's note: further work is required to elaborate this section.

9.1 Requirements for extensions or additions to NGN capabilities

9.1.1 Requirements for numbering, naming and addressing (NNA)

Based on the service requirements in clause 8.12, NGN is required to support the following additional NNA requirements.

- 1) NGN is required to provide the addressing mechanism according to the operator's policy.
- 2) A static MOC group contains the members of MOC entities which are pre-configured.
- 3) A dynamic MOC group is generated by certain criteria when requested, such as: location, status of MOC entities, etc.
- 4) The MOC group may contain the MOC entities (e.g. MOC devices) which are directly or indirectly connected to NGN.

5) NGN is required to map the MOC group identifier to network addresses of MOC entities of a static MOC group.

6) NGN is required to identify the list of MOC entities and their network addresses matching the specified criteria for dynamic MOC group.

9.1.2 Quality of service

9.1.2.1 QoS policy for group

Based on the service requirements in clause 8.12, NGN is required to support per group level QoS policy, in parallel to, or instead of, per user level QoS policy.

The per group QoS policy parameters include (but are not limited to):

- packet transfer delay
- packet delay variation
- packet loss ratio
- packet error ratio

9.1.2.2 Traffic control

Based on the time controlled network communication requirements defined in clause 8.2, the following additional requirements are placed on NGN:

1) NGN is required to allow MOC end users' access (e.g. attach to the network or set up a data connection) during a defined granted network communication access time interval.

2) NGN is required to reject MOC end users' access (e.g. attach to the network or set up a data connection), or allow it with different charging parameters, during a defined forbidden network communication access time interval.

3) NGN is required to allow modification of granted network communication access time intervals based on service criteria (e.g. daily network traffic load, MOC device location).

4) NGN is required to communicate granted network communication access time schedules and durations to MOC devices.

5) NGN is required to terminate MOC end users' access (e.g. detachment from the network or disconnection of a data connection) when a network communication access time duration has ended.

6) NGN can optionally support the communication of granted network communication access time schedules and durations to other MOC end users than the MOC devices (e.g. MOC application server).

Based on resource usage requirements in clause 8.3, the following additional requirements are placed on NGN:

1) NGN is required to page on the target device before service interaction when the network needs to initiate a service.

2) NGN is required to establish resources only when transmission occurs.

Based on requirements in clause 8.12, in addition to the existing NGN traffic control capabilities, NGN is required to support:

1) optimized handling of group communications in order to save network resources and to prevent network congestions.

2) per group level traffic control in parallel to, or instead of, per user level traffic control. The per group level traffic parameters include (but are not limited to):

- maximum allowed packet size
- data rate and the bucket size
- peak rate and peak bucket size
- sustainable rate and sustainable bucket size

9.1.3 Accounting and charging

Based on the service requirements in clause 8.12, NGN is required to support group-based accounting and charging either for both on-line charging and off-line charging in parallel to, or instead of, per device level charging.

9.1.4 Mobility handling

Based on mobility levels in clause 8.1, the following additional requirements are placed on NGN:

- 1) NGN is required to support different mobility level management according to the mobility requirements of MOC devices.
- 2) NGN is recommended to support dynamical instruction of the MOC devices in order to set the mobility level (implying for example the adjustment of the frequency of mobility management procedures).

Editor's note: It should be also clarified how the NGN knows the required mobility level. Use cases of mobility handling could be useful to understand this requirement.

9.1.5 Profile management

Based on the management requirements in clause 8.9, the following additional requirements are placed on NGN:

9.1.5.1 User profile management

Based on the service requirement in clause 8.9.2, the following requirement is placed on NGN:

- 1) NGN is recommended to support a standard set of MOC service profiles.

9.1.5.2 Device profile management

Based on the service requirement in clause 8.9.3, the following requirement is placed on NGN:

- 1) NGN may support device profiles which contain MOC device and MOC gateway information sets.

9.1.6 Device management

Based on the service requirements in clause 8.9.1, NGN is required to support the following additional device management requirements:

- 1) NGN is required to be able to monitor the MOC devices and gateways for various aspects and report the running situation of MOC device and gateway, including:

- a. monitor the behaviours of MOC devices which are not aligned with subscribed service feature(s);
- b. change of the association between the device and the UICC(Universal Integrated Circuit Card);
- c. change of the network point of attachment of MOC devices and gateways;
- d. MOC devices and gateways' loss of network connectivity.

9.2 Requirements supported by existing NGN capabilities

Based on the service requirements in clause 8, this clause specifies requirements supported by existing NGN capabilities.

9.2.1 Group management

NGN provides group management specified in clause 8.12 are supported by the existing group management capabilities of NGN [ITU-T Y.2201].

9.2.2 Quality of service

9.2.2.1 Differentiated quality of service and data prioritization

NGN provides QoS supporting capabilities in terms of differentiated quality of service and data prioritization. The differentiated quality of service and data prioritization requirement specified in clause 8.13 is supported by the existing capabilities of NGN [ITU-T Y.2201, ITU-T Y.2221].

9.2.3 Location management

NGN provides location management capability which determines and reports information regarding the location of users and devices within the NGN. The location management requirements specified in clause 8.11 are supported by the existing location management capabilities of NGN [ITU-T Y.2201].

9.2.4 Mobility

NGN provides mobility support for the NGN. The mobility requirements specified in clause 8.1 are supported by the existing capabilities of the NGN Release 1 [ITU-T Q.1706].

9.2.5 Security

NGN provides security capabilities. The service requirements specified in clause 8.14 are supported by the existing security capabilities of NGN [ITU-T Y.2201] and [ITU-T Y.2701].

9.2.6 Addressing and identification

NGN provides addressing and identification capabilities. The service requirements specified in clause 8.10, 8.12 are supported by the existing capabilities of NGN [ITU-T Y.2201] and [ITU-T Y.2702].

9.2.7 Accounting and charging

NGN provides accounting and charging capabilities. The service requirement specified in clause 8.8 is supported by the existing capabilities of NGN [ITU-T Y.2233].

9.2.8 Communication mode

Based on the service requirements in clause 8.12, NGN is required to support the following communication modes for MOC groups which contain MOC entities directly or indirectly connected to NGN:

- anycast
- multicast
- broadcast

These requirements are supported by the existing capabilities of NGN [ITU-T Y.2201].

10 MOC device domain capability requirements for support of MOC applications

Editor's note: each sub-clause should be ordered according to 1) common requirements to both MOC gateway and MOC devices, 2) requirements specific to MOC gateway and to MOC devices

Editor's note: the requirements of MOC devices in this clause may not be applicable to all possible types of MOC devices. Further consideration is necessary to clarify this point.

10.1 Application Enablement

MOC gateway may support the effective hiding of MOC devices' operations to the MOC applications.

Editor's note: it should be identified that what service requirement are based on by the following capabilities requirements.

Based on the service requirements in clause 8.5, the following requirements apply to the MOC gateway and MOC device capabilities:

- 1) MOC gateway can optionally support a set of abstracted operations on MOC devices.
- 2) MOC devices are recommended to support a set of abstracted operations.
- 3) MOC gateway can optionally support the implementation of service logic to provide MOC capabilities.
- 4) MOC devices are recommended to support the implementation of service logic to provide MOC capabilities.

10.2 Mobility

Based on the requirements in clause 8.1, the following requirements apply to the MOC gateway and device capabilities:

- 1) MOC gateway and MOC devices are required to support enhanced mobility management capabilities in order to support different levels of mobility.

10.3 Communication

Based on the requirements in clause 8.2, 8.3, 8.5, the following requirements apply to the MOC gateway and MOC device capabilities:

- 1) MOC gateway is required to select the proper routing paths between the traffic originating endpoint and the traffic receiving endpoint.
Editor's note: to elaborate on various endpoint examples.
- 2) MOC gateway is required to allow setting and modification of granted network communication access time schedules and durations. *Editor's note: to see if there is an impact on the gateway concerning "MOC applications require that (granted/forbidden) network communication access time schedules and durations are communicated to the MOC devices."*
- 3) MOC gateway and MOC devices are required to be able to establish, maintain or release communication resources according to the data communication needs.
- 4) MOC gateway is required to support the following communication modes according to the service requirements:
 - anycast
 - multicast
 - broadcast
- 5) MOC gateway is required to support interworking with legacy MOC devices (e.g., devices with proprietary standards for inter-working with network entities).
- 6) MOC devices can optionally communicate with the network based on service criteria (e.g. daily network traffic load, MOC device location, access time schedules and durations).
- 7) MOC devices are required to be turned offline (i.e. no active connection) when no data transmission is required.

10.4 QoS

Based on the requirements defined in clause 8.2, 8.13, the following requirements apply to the MOC gateway and MOC device capabilities:

- 1) MOC gateway is required to support the traffic control policy which defines granted network communication access time schedules and durations.
- 2) MOC gateway is required to support QoS differentiation over various categories of traffic.
- 3) MOC gateway is recommended to support service/application priority
- 4) MOC gateway is required to provide performance measurement and management.
- 5) MOC devices are required to support the traffic control policy which defines granted network communication access time schedules and durations.
- 6) MOC devices are required to support QoS differentiation over various categories of traffic.
- 7) MOC devices are recommended to support service/application priority
- 8) MOC devices are required to provide performance measurement and management.

10.5 Remote management

Based on the requirements in clause 8.9.1, the following requirements apply to the MOC gateway and MOC device capabilities:

- 1) MOC gateway is required to act as a management proxy for MOC devices of the MOC local network, such as accept and process management requests from NGN, to perform local (to the MOC local network) firmware/software and management update.
- 2) MOC gateway is required to perform software and firmware update of itself.
- 3) MOC gateway is required to support configuration management
- 4) MOC gateway is required to support collecting and storing performance and fault related data.
- 5) MOC devices are required to perform software and firmware update of itself.
- 6) MOC devices are required to support configuration management
- 7) MOC devices are required to support collecting and storing performance and fault related data.

10.6 Addressing

Editor's note: this clause needs alignment with clause 8.10.

Based on the requirements in clause 8.10, 8.12, the following requirements apply to the MOC gateway and MOC device capabilities:

- 1) MOC gateway is required to support mapping between the identity of a MOC device and one or more local area network addresses.
- 2) MOC gateway is required to support mapping between the identity of a MOC device group and one or more local area network addresses for each MOC device within the group.
- 3) MOC devices are required to be addressable.
- 4) MOC devices are required to support of unique identification.

10.7 Security

Based on the requirements in clause 8.14, the following requirements apply to the MOC gateway and MOC device capabilities:

- 1) MOC gateway is required to support secure transport mechanisms, such as encryption and integrity protection.
- 2) MOC devices are recommended to support secure transport mechanisms, such as encryption and integrity protection.
- 3) MOC gateway and MOC devices are required to support registration and authentication with the MOC applications.

10.8 MOC device identifier management

Based on the requirements in clause 8.12, the following requirements apply to the MOC gateway capabilities:

- 1) A MOC gateway can optionally use temporary identifiers for MOC devices connecting and disconnecting to the network dynamically.
- 2) A MOC gateway can optionally re-appoint dynamically released temporary identifiers to other MOC devices.

10.9 Charging

Based on the requirements in clause 8.8, the following requirements apply to the MOC gateway capabilities:

- 1) MOC applications are recommended to support different charging and accounting methods for the MOC devices which are connected to the MOC gateway.

11 Reference framework for MOC capabilities

Editor's note: this clause should provide a reference framework for the operation of MOC capabilities in NGN environment.

Editor's note: The approach followed in Y.2240 (specifically, the NGN-SIDE framework) should be considered and appropriate relationship developed (e.g. distinction between common (NGN-SIDE) and MOC specific capabilities in the NGN domain).

Editor's note: the reference framework for MOC capabilities will build on the requirements and capabilities identified for the support of MOC applications in NGN (clauses 8 and 9 of this draft Recommendation) and will be input to detailed functional developments (functional architecture for MOC)

11.1 High level view

Figure 11.1 provides a high level view of the reference framework for MOC capabilities

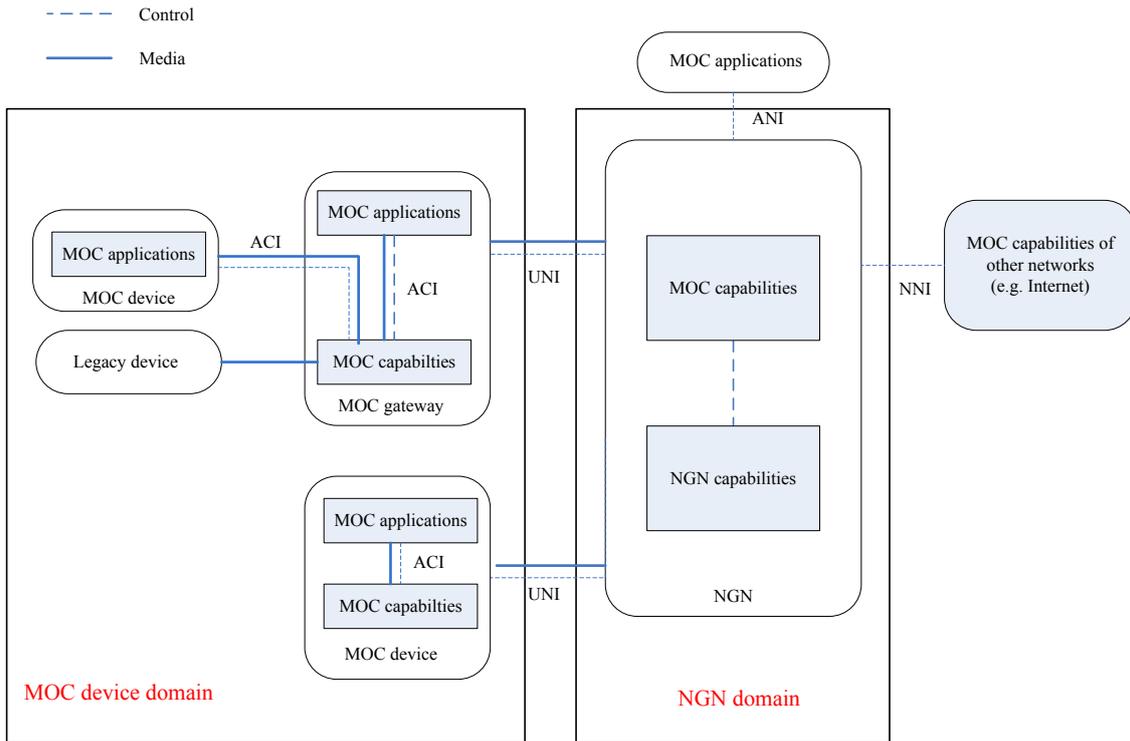


Figure 11.1 High level view of the reference framework for MOC capabilities

- The MOC device domain is composed of MOC devices and MOC gateways. MOC capabilities of the MOC device domain collaborate with MOC capabilities and NGN capabilities of the NGN domain to support MOC applications.
- The NGN domain is composed of:
 - NGN capabilities;
 - MOC capabilities;

Editor's note: it should be further considered if some of the MOC capabilities in 11.2 and 11.3 can be equivalent to other (NGN) service platform level capabilities described in other approved Recommendations (e.g. Y.2240).

11.2 MOC capabilities in the NGN domain

The MOC capabilities in the NGN domain are shown in figure 11.2. NOTE - the functional entities corresponding to the MOC capabilities in the NGN domain are positioned inside the NGN service stratum [ITU-T Y.2012].

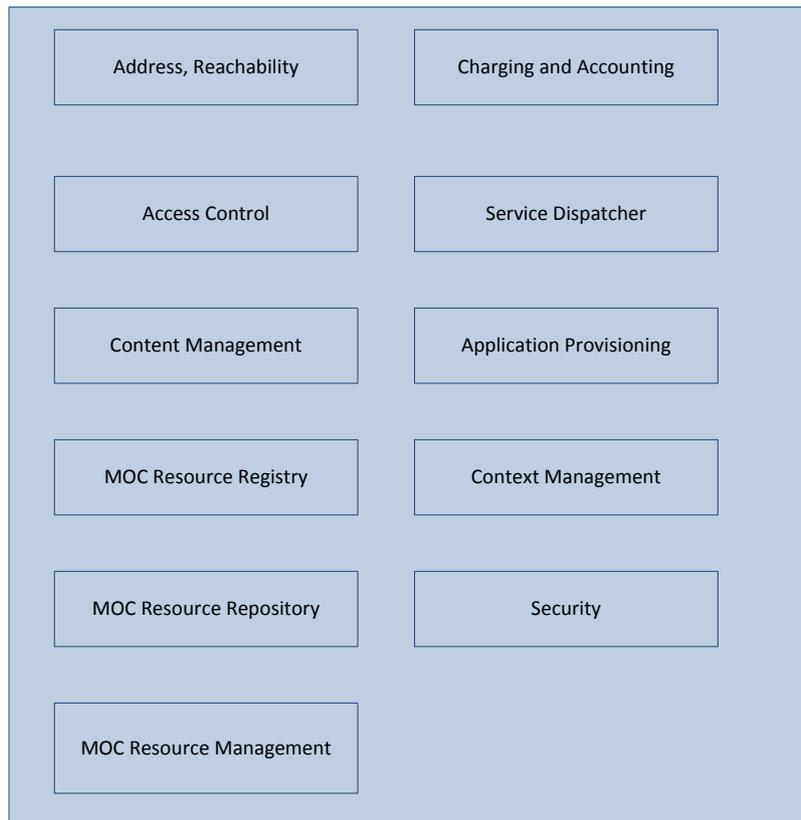


Figure 11.2 MOC capabilities in the NGN domain

11.2.1 Charging and accounting

The charging and accounting capability is required to support charging modes and mechanisms as specified in [ITU-T Y.2233], including:

- Support of revenue sharing among the various actors involved in the MOC ecosystem;
- Support of event-based online/offline charging in the MOC ecosystem.

11.2.2 Access control

The access control capability performs authentication and authorization of MOC applications before allowing them to access a specific set of capabilities. The access control capability provides translation of APIs/protocols across different service interfaces as well as access from applications to functionalities exposed by MOC capabilities.

11.2.3 Service dispatcher

The service dispatcher capability provides unified message routing and message exchange mechanisms within MOC capabilities in NGN.

The message routing mechanisms provide route calculation for requests and responses between MOC applications and MOC devices and gateways. Message routing can be based on various criteria, e.g. context, policies.

The message exchange mechanisms control the message flow between MOC applications and MOC devices and gateways.

The service dispatcher also provides API and protocol transformation from MOC applications to common message structure and business event handling and vice versa.

11.2.4 Content management

Content management can be provided as resources to MOC application or customer by different MOC resource providers (e.g. content providers and end users).

The content management capability provides extraction of appropriate information (including size, type, location) from content, enabling the MOC service platform to ensure the integrity of the content itself.

The content management capability provides profiling of content as appropriate to enable its delivery to different MOC applications, such as content for specific applications, content for specific customer.

The content management capability provides dispatching of content in order to expose content to applications.

11.2.5 Application provisioning

The application provisioning capability is used for deployment of applications in a secure way by the MOC application provider when they are available for deployment. This capability provides application packaging, publishing, deployment, lifecycle management and monitoring functions.

11.2.6 Context management

The context management capability collects, aggregates and manages context information related to different context sources, exposing context information, including to other MOC capabilities, according to the MOC application provider's policies.

11.2.7 MOC resource registry

This capability provides the functionalities related to the registration, deregistration, discovery, and governance of resources offered by MOC resource providers. Registration-oriented resource descriptions including unique resource identification and resource addressing are published in MOC resource registry.

This capability defines a mechanism for a resource of a MOC resource provider to be registered within the MOC service **platform**, so that this resource can be located and accessed by applications.

11.2.8 MOC resource repository

The MOC resource repository capability is required to provide functionalities for the storage of information related to the registered MOC resources. By storing in the MOC resource repository, the MOC resource information can be accessed by the authenticated and authorized MOC

applications. Information related to the registered resources includes various suitable packaging tools (e.g. Java SDK, .NET SDK and Eclipse) for application developers.

11.2.9 MOC resource management

The resource management capability performs the controlling functions for MOC resources in order to satisfy the MOC applications' requirements.

MOC resource management capability is recommended to support configuration management, fault management, performance management, software and firmware upgrade of MOC devices or MOC gateways.

11.2.10 Addressing, reachability

The addressing capability provides a unique mapping between the identity of MOC devices (MOC gateways, group of MOC devices and MOC gateways) and a set of MOC device related information (e.g. location, policy, access rights).

The reachability capability provides dynamic information concerning the reachability status of MOC devices (e.g. online/offline, forwarding information)

The information provided by the addressing and reachability capabilities should be accessible to other capabilities.

11.2.11 Security

The security capability performs mutual authentication between MOC devices/gateways and the MOC service platform. The security capability provides encryption/integrity protection on data exchanged between the MOC devices and gateways and the MOC service platform to ensure secure delivery when security is required.

11.3 MOC capabilities in MOC device domain

Editor's note: content of this clause needs detailed review.

The MOC capabilities in the MOC device domain are shown in figure 11.3.

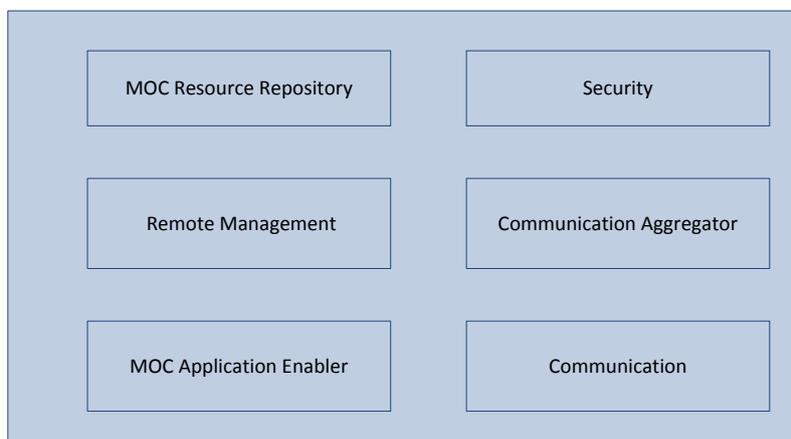


Figure 11.3 MOC capabilities in the MOC device domain

11.3.1 Communication aggregator

The communication aggregator capability residing in MOC gateway provides generic communication and performs proxy and traffic aggregator functions.

The Communication aggregator capability supports relaying traffic between MOC device and NGN, QoS mechanism based on the service policy, recording charging information for the device within MOC local network

11.3.2 MOC Application enabler

MOC application enabler capability performs the exposure of MOC capabilities of the MOC gateway and MOC devices, hiding the service capabilities of the MOC gateway and MOC devices.

11.3.3 MOC resource repository

The MOC resource repository capability in MOC gateway provides functionalities for the storage of information related to the registered MOC devices. By storing in MOC device repository, the MOC devices' data can be read by the authenticated and authorized MOC applications.

11.3.4 Remote management

The MOC remote management capability performs the controlling functions for MOC gateway and MOC devices in order to satisfy the application's requirements.

The MOC remote management capability supports configuration management, fault management, performance management, software and firmware upgrade of MOC gateway and MOC devices in MOC local network.

11.3.5 Security

The security capability performs registration and mutual authentication with MOC applications.

The security capability provides encryption/integrity protection on data exchanged with the NGN, MOC applications and MOC gateway to ensure secure delivery when security is required.

The security capability performs key management based on the service keys generated in MOC devices, and protects from unauthorized applications' access to the MOC devices.

11.3.6 Communication

The communication capability performs the generic communication functions in MOC devices.

The communication capability provides secure application data transport functions, such as encryption and integrity protection, delivers messages to MOC applications or receives messages from MOC applications in accordance with the service criteria (e.g. daily network traffic load, MOC device location, access time schedules and durations), and handles these messages.

11.4 MOC Service interfaces

The MOC service interfaces support:

- MOC applications hosted in MOC devices and gateways, which access NGN via UNI ;
- MOC applications hosted in MOC gateways and MOC devices, which access the MOC capabilities hosted in MOC gateway via Application Capability Interface (ACI);
- MOC applications hosted in MOC devices, which access the MOC capabilities hosted in those same MOC devices via Application Capability Interface (ACI);
- MOC applications hosted by 3rd parties, which access NGN via ANI.

MOC applications hosted in MOC devices and gateways can be invoked by MOC service customers and other MOC applications, e.g. MOC applications hosted by 3rd parties.

MOC service interfaces are recommended to implement standardized APIs, protocols, and technologies to realize the service exposure towards MOC applications.

11.4.1 Service interface requirements across ACI

ACI service interface is used to provide interaction between MOC capabilities of devices and gateway and MOC applications of devices and gateway. ACI service interface allows an application residing in a MOC device to access MOC capabilities in the same MOC device or in a MOC gateway. It also allows an application residing in a MOC gateway to access MOC capabilities in the same MOC gateway.

ACI is required to support the following functions:

- Registration of MOC devices and MOC gateways to the MOC capabilities in MOC device and gateway (e.g. registration of a sensor or GPS in a car to the gateway in the car).
- MOC applications' execution requests of MOC device-specific tasks by a MOC device and gateway or group of MOC devices and gateways.
- Subscription and notification to specific events (e.g. mutual subscription and notification to specific events (e.g. connectivity of MOC devices and gateways) between MOC capabilities and applications).MOC device and gateway's requests of creation, deletion and members' listing of a group.

11.4.2 Service interface requirements across UNI

UNI service interface is used to provide interaction between MOC capabilities of MOC devices and gateway and MOC capabilities of the NGN. UNI is recommended to support standardized APIs for exposing MOC resources and functions to applications. UNI is required to support the following functions:

- Registration of MOC capabilities in the MOC device domain to MOC capabilities in the NGN domain.
- Request of the execution of a specific task to be performed by a MOC application.
- Subscription and notification to specific events.

- Requests of the creation, deletion and members' listing of group(s).

11.4.3 Service interface requirements across ANI

The service requests initiated by MOC applications are sent to the MOC service platform via ANI. ANI allows a MOC application to access the MOC capabilities. ANI service interface is required to provide the interaction between 3rd party applications and MOC capabilities of NGN. ANI is recommended to support standardized APIs at the ANI for exposing MOC resources to MOC applications.

ANI is required to support the following functions:

- Registration of MOC applications to the MOC capabilities in NGN domain.
- Request of the execution of a specific task to be performed by a MOC device and gateway or group of MOC devices/gateways.
- Subscription and notification to specific events
- Requests of the creation, deletion and members' listing of group(s).

11.4.4 Service interface requirements across NNI

NNI service interface is used to provide interaction with MOC capabilities of other networks. The following service interfaces are relevant for the interaction of NGN with MOC capabilities of other networks at NNI level:

- Service interface between NGN and other networks (NGNs or non-NGNs), both having capabilities for support of MOC applications.

NOTE - the scenario of NNI interaction between NGN and other networks which have no capabilities for support of MOC applications is not applicable as it is only from a network transport interface perspective.

Appendix I

MOC use cases

(This appendix does not form an integral part of this Recommendation)

I.1 e-Health

Editor's note: The following description for e-Health use case may need further work to elaborate it more clearly and identify specific attributes of this MOC use case.

e-Health is a relatively recent term for healthcare practice supported by electronic processes and communication. Figure I.1 shows the example of e-Health service configuration. There are various types of devices involved, such as body parameters measuring sensors, GPS-capable devices, cameras, or even gateways, etc. Some of them only collect data and send it to network in single direction (e.g. heart beat sensor), some of them can interact with network in bi-direction (e.g. camera), some of them usually generate small amount of data (e.g. thermometer), some of them may involve multimedia streaming (e.g. camera), some of them may involve call session control (e.g. SIP terminal supporting voice/video call) and some of them can even work as both gateway and providing sensor-like services. The devices gather the data and send them to the services provider. Hospital, doctor and family can subscribe the service to get raw data or result information processing from raw data.

Devices on or around patient can access to communication network directly or via gateway(s) (e.g., home gateway or gateway worn on body),

- 1, when the patients stay in indoor environment, devices can access network via one single gateway or dynamic gateways which mean that patients can move between gateways and access network based on different gateways respectively.

- 2, when the patients roam outside, the devices on the body can access to network via mobile network directly or via the gateway on body.

The following technical challenges need to be considered:

- Grouping feature should be supported by the service, for instance, patients with the same type of disease. For one patient, he/she may have a group of devices which can be managed in group way.
- Optimized traffic control should be supported by the service. For instance, detected of data may be very small and reported to network every one hour. In that case, it is a waste of resource for a patient to connect to network consistently and the network can be optimized for low traffic, for example, traffic can be delivered through user plane signalling and there is no need to provide data-dedicated IP bearer. Additionally, devices on patient maybe in sleepy mode in some cases, for instance, the devices will be in sleepy mode and will be waked up when the doctor needs to diagnose the patient remotely. Thus,
- Different mobility lever should be supported by the service. For instance, the patient usually has low mobility since they may be very weak and don't move in large areas frequently. In that case, it is a waste of resource if high mobility management is provided.

Devices on patient maybe in sleepy mode for some cases, for instance, the devices will be in sleepy mode and will be waked up when the doctor needs to diagnose the patient remotely.

- The service is required for supporting time control. For instance, devices on patient may collect a lot of data but it doesn't mean that they have to report instantly each time after they collect the data, if the data is not very crucial and is just for routine examination of health. For this kind of

scenario, the network can allocate some certain time slots for the devices to report data which means that the devices can not report data during other moment or will be charged in higher rate.

- Device profile should be supported by the service. Patient may buy new devices and add them to network dynamically, and network should be able to authenticate and control the newly-added devices and remove the devices from network vice versa.
- Device behind the MOC gateway should be identified by the network. MOC gateway may just provide a bear channel and act as a data aggregator for devices connected to it or may provide service control for the devices connected to it. When a gateway acts as a data aggregator and provides bear channel, devices connected to the gateway should be controlled by network, or else the devices may be controlled by both network and gateway.
- Legacy device should be supported by the service. E-Health is not a brand new term and has been existing for a long period; there are plenty of legacy devices or gateways running in networks which are not compliant with well-defined standards, for instance, USN or MOC. The MOC should be able to support backward compatibility or adaptation to existing legacy devices or gateways.

Patients usually are not very familiar with pros and cons of different hospitals, they can just logon the operator's or e-health centre's portal and subscribe services, whereas e-health centre usually are familiar with it and they can determine the target serving hospitals (one or multiple hospitals) for the patients based on their professional knowledge. There might have one or multiple hospitals providing medical service to the patient jointly. Hence, when the devices on patient report data to the e-health centre can intelligently help the patients to select the best target doctors or hospitals, and route the data to one or multiple hospitals for joint diagnosis. And multimedia call control session might be needed in this scenario, including audio, video, text chatting, etc. Service profile should be supported by the service. Device should also interact with multiple applications.

When doctors diagnose and provide health care services remotely, they usually also need the existing hospital internal disease diagnostics system or database system to assist, for example, data reported from devices maybe input to existing hospital internal system, in this case, the devices should be interoperable with existing systems, for example, data format, service capabilities invoke, etc., which indicates that the MOC e-Health system should be able to collaborate and inter-work with the existing service\application system which is usually heterogeneous.

- Traffic load balance should be take into consider for the complicated situation. For instance the population distribution of patients may vary. For instance, there may have relatively higher rate of patients in gerocomium or some old communities or in some certain cities, while lower in some other areas or cities. The network should support system imbalance handling for high traffic or service load accordingly, especially for video-like services, for example, when many patients use remote video diagnosis, the network may have to endure heavy traffic load.

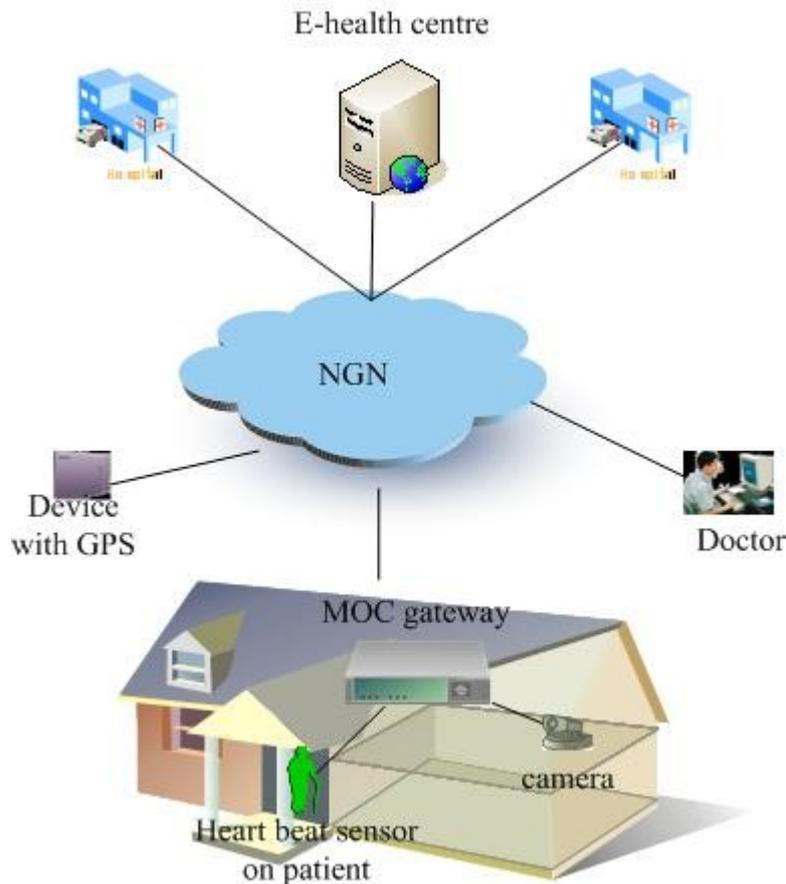


Figure I.1 e-Health service configuration

Editor's note: The use cases I.2 to I.7 have not been reviewed in detail, further review is required.

I.2 Tsunami warning service

Tsunami warning system is used to detect tsunamis and issue warnings to prevent loss of life and property. As shown in figure I.2, It consists of two equally important components: a network of sensors to detect tsunamis and a communications infrastructure to issue timely alarms to permit evacuation of coastal areas. Detection and prediction of tsunamis is only half the work of the system. Of equal importance is the ability to warn the populations of the areas that will be affected. All tsunami warning systems feature multiple lines of communications (such as SMS, e-mail, fax, radio, text and telex, often using hardened dedicated systems) enabling emergency messages to be sent to the emergency services and armed forces, as well to population alerting systems (e.g. sirens). In this use case, the service is required to support:

- Inter-working with heterogeneous network, including: mass media network (e.g. radio network, TV network), dedicated communication system (e.g. sirens)
- Delivery of emergency data over unreliable bearer, e.g., to support communication through satellite system.
- System robustness. i.e., the system should support data bursting within a short while due to large number of machines within an area.
- Prioritized service level. i.e., the message for earthquake should be prioritized comparing with other service messages.

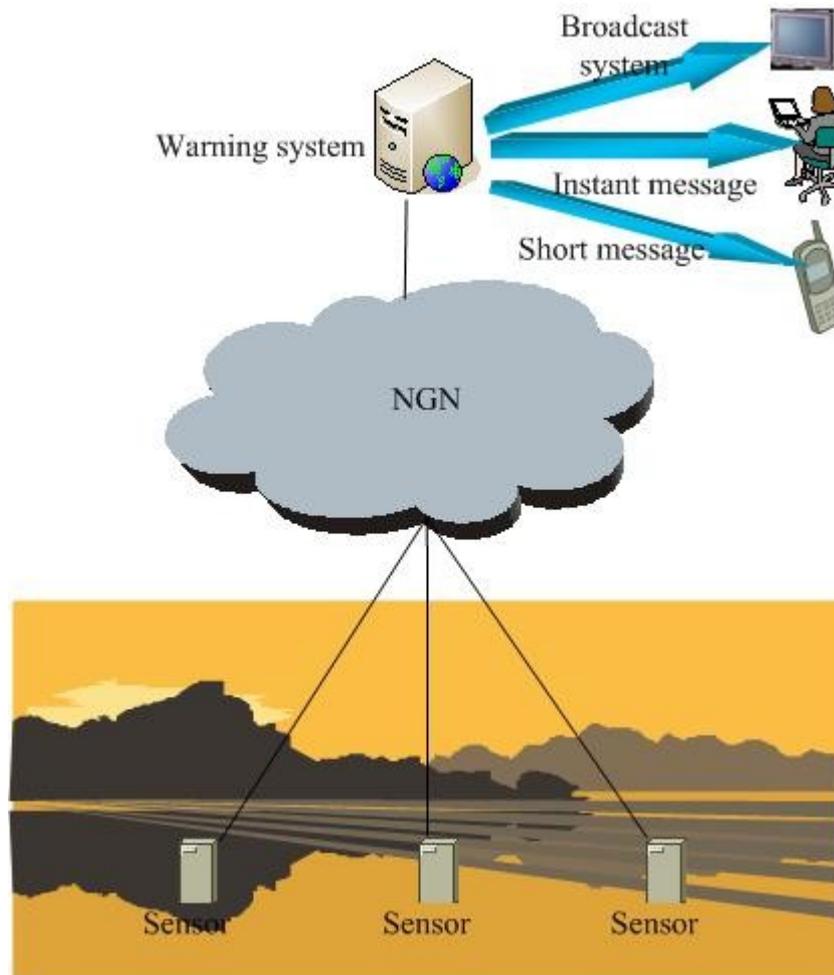


Figure I.2 Tsunami warning service configuration

I.3 Motorcade Management

As shown in figure I.3, the control centre gathers the data of location, speed and situation from the sensor, GPS and the cameras in a bus which access wireless network through gateway. The dynamic time table pushes on the screen of bus stop. When sensor detects something out of normal situation, like gasoline, an alarm indication will be sent to the centre. Because the bus should moves in a certain region, services should be triggered, for example a call may be made to the bus driver or an alert indication be pushed to the driver, if bus moves out of the region. In this use case, the NGN should support:

- Low mobility, move only within a certain region
- Location based service: network or application trigger services when devices are in a particular area.
- Prioritized service level. For example, the alarm message should be prioritized comparing with other data.
- Group management for machines with same characteristics.

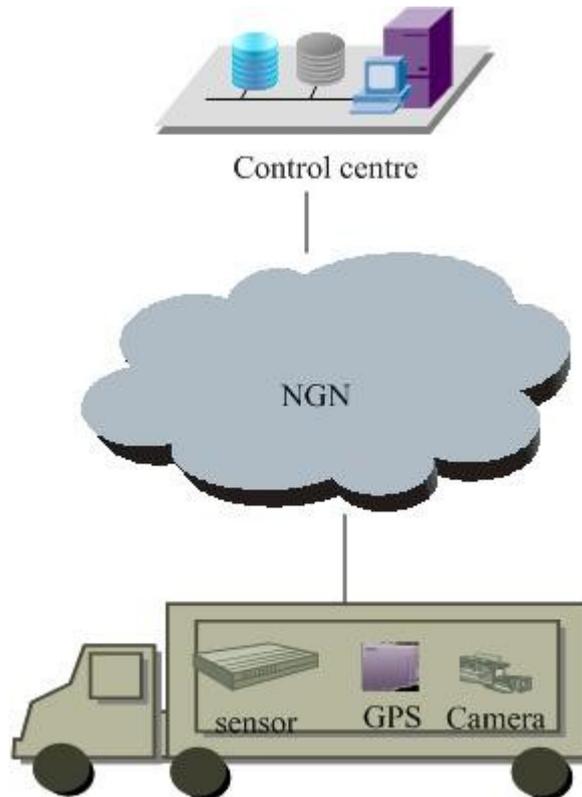


Figure I.3 Typical Motorcade Management service configuration

I.4 Oil well monitor

Editor's note: it is for consideration to delete this use case if no specific requirements are identified (e.g. e-health)

The camera collects the environmental information of the oil well, the meters and the sensors collect the status information of the oil well. Oil wells always locate in an open country, so these devices usually access network through wireless network..

In this use case, the NGN should support:

- Device monitor: if connectivity is loss, the state of devices should be changed
- Group management for machines with same characteristics.

I.5 Patrol and surveillance

Editor's note: it is for consideration to delete this use case if no specific requirements are identified (e.g. e-health)

Polices and prisoners pull on RFID in prison. Control centre gathers patrol information of polices and position of prisoners via RFID reader. If a prisoner access places without permission, the video of this place will show on the monitor screen. In this use case, the NGN should support:

- Low mobility, move only within a certain region
- Location based service: network or application trigger services when devices are in a particular area.
- Service interaction: location service interact with video surveillance

I.6 Smart metering

A smart metering scenario often refers to devices (e.g. valves, electricity meters, gas meters, water meters, ...) which are connected to a data centre via a gateway (figure I.4). The data centre collects data from the devices and is able to control relevant devices remotely via the gateway.

Smart Metering usually involve a different technology mix, such as real-time or near real-time sensors, power outage notification, and power quality monitoring. These additional features are more than simple automated meter reading (AMR). They are similar in many respects to advanced metering infrastructure (AMI) meters. Smart metering are also believed to be a less costly alternative to traditional interval or time-of-use meters and are intended to be used on a wide scale with all customer classes, including residential customers. Interval and time-of-use meters are more of a legacy technology that historically have been installed to measure commercial and industrial customers, but typically provide no AMR functionality. Smart metering may be part of a smart grid, but alone do not constitute a smart grid.. In this use case, the NGN should support:

- High compatibility to inter-work with existing deployed (legacy) machine to machine network either in terminal and access layer or in network and service layer since the existing deployed systems are usually based on industry-defined standards.
- Unified service and charging model since both electricity and telecommunication are usually indispensable for consumers. i.e., there is only one unified charging table for one consumer to reflect electricity fee and telecommunication fee his/her family has used over the past month.
- Group management for machines with same characteristics.
- Message broadcasting and multicasting based on specific characteristics, such as group, location, etc., to support functions for instance firmware upgrading, etc.
- Distributed MOC service platform to provide high availability and better load balance

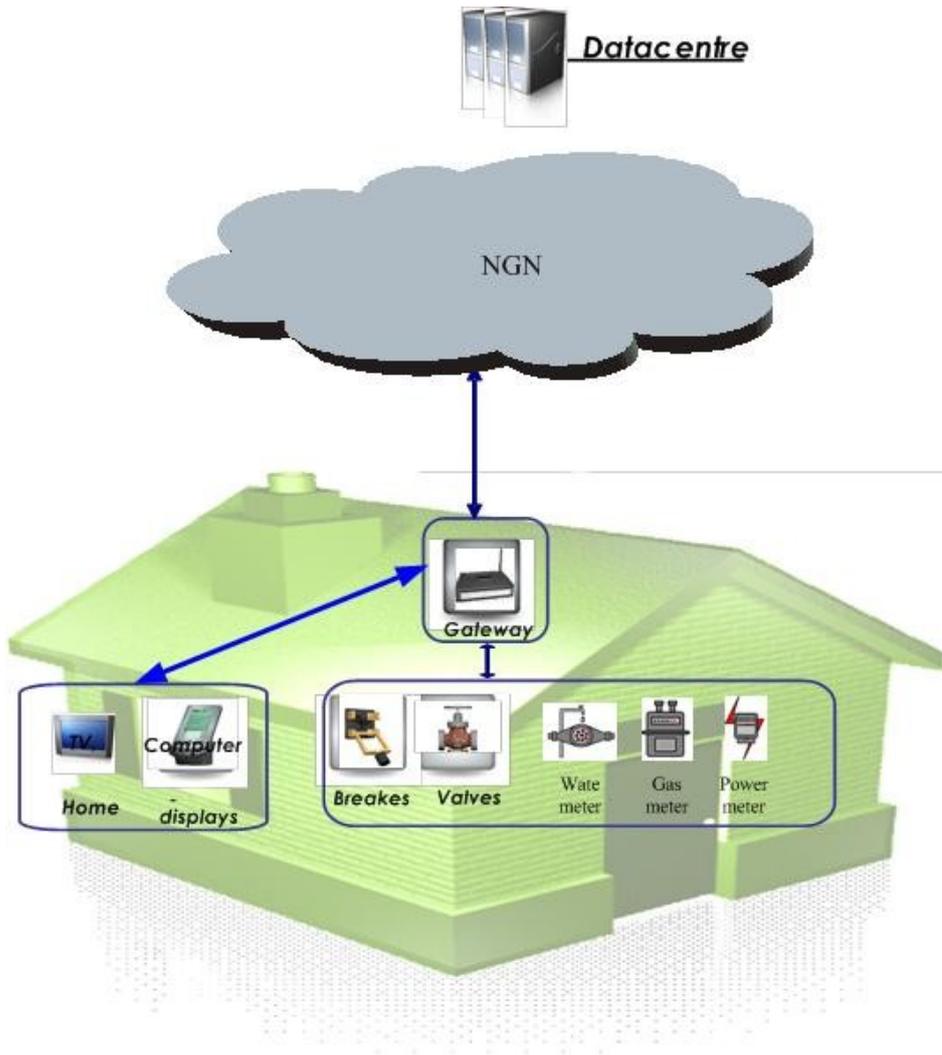


Figure I.4 Typical Smart Metering service configuration

I.7 Video surveillance

Video surveillance has been a popular security tool for years. And due to new breakthroughs in technology, security cameras are more effective than ever before. Banks, retail stores, and countless other end-users depend on the protection provided by video surveillance. While analog CCTV systems were once the norm, they can be expensive, requiring complicated installations and constant upkeep. Fortunately, advances in digital technology have made video surveillance systems far more cost-effective, flexible, and simple to operate. Security systems using IP (Internet Protocol) cameras are easy to install and maintain, and can be customized and scaled to perfectly match customer's specific needs.

IP-based video surveillance is widely predicted to be the way of the future, and network cameras are now readily available – in packages, bundled together with software and support, or on their own. With most IP camera systems, all customers' need to do is choose where they want the cameras, and plug them in – it's that easy! IP cameras come in so many varieties that choosing the right models may seem daunting. In Machine-oriented communication environment, video surveillance is a indispensable part of services.

- NGN should support enhanced video/audio based services, such as concurrent video streaming, local-breakout, etc.

I.8 Smart home

Editor's note: 1) the text should be organized with figure and then detailed description associated with the figure. Also, it should be clarified 2) if this use case is related to one or more specific type (types) of communication, 3) the associated requirements similarly to existing use cases in the current draft.

Editor's note: it would be useful to describe more the use cases in terms of possible business models (and consequently review the related business models clause in the body).

Tom's house is a **smart home** with MOC devices (*Editor's note: what are these? Fire sensors, door break-out sensors, power, gas, water sensors, cameras...*) which is managed by the **MOC service platform (SP)**. Tom's house information related to power, gas and water consumption can be collected and reported to the **MOC SP**. At the same time, Tom can manage **policy** information of his home's MOC devices in the **MOC SP** and the policy can be sent to MOC devices and executed intelligently.

Tom defines the policy as follows:

- 1) if a fire sensor detects signs of a fire in Tom's house, then the fire sensor shall send a short message alarm to Tom's mobile phone;
- 2) if an alarm is triggered by a door break-out sensor then a video communication is initiated allowing Tom to see in real time what is happening in his house.

Let us assume that a thief breaks out one door of Tom's house. When detecting this event, the MOC device (i.e. the door break-out sensor) initiates a video communication between Tom and a visual surveillance camera located in Tom's home. Tom watches and records the video in his mobile, record which may be used as a **proof**.

Let us now consider that Tom is out of his house while a fire occurs in his home's kitchen where his son is cooking. When detecting this event, the MOC device (i.e. the fire sensor) sends an alarm message to Tom directly. Upon reception of this information, Tom initiates a video communication with the MOC device to check the status of the kitchen, and to tell his son how to use the fire extinguisher.

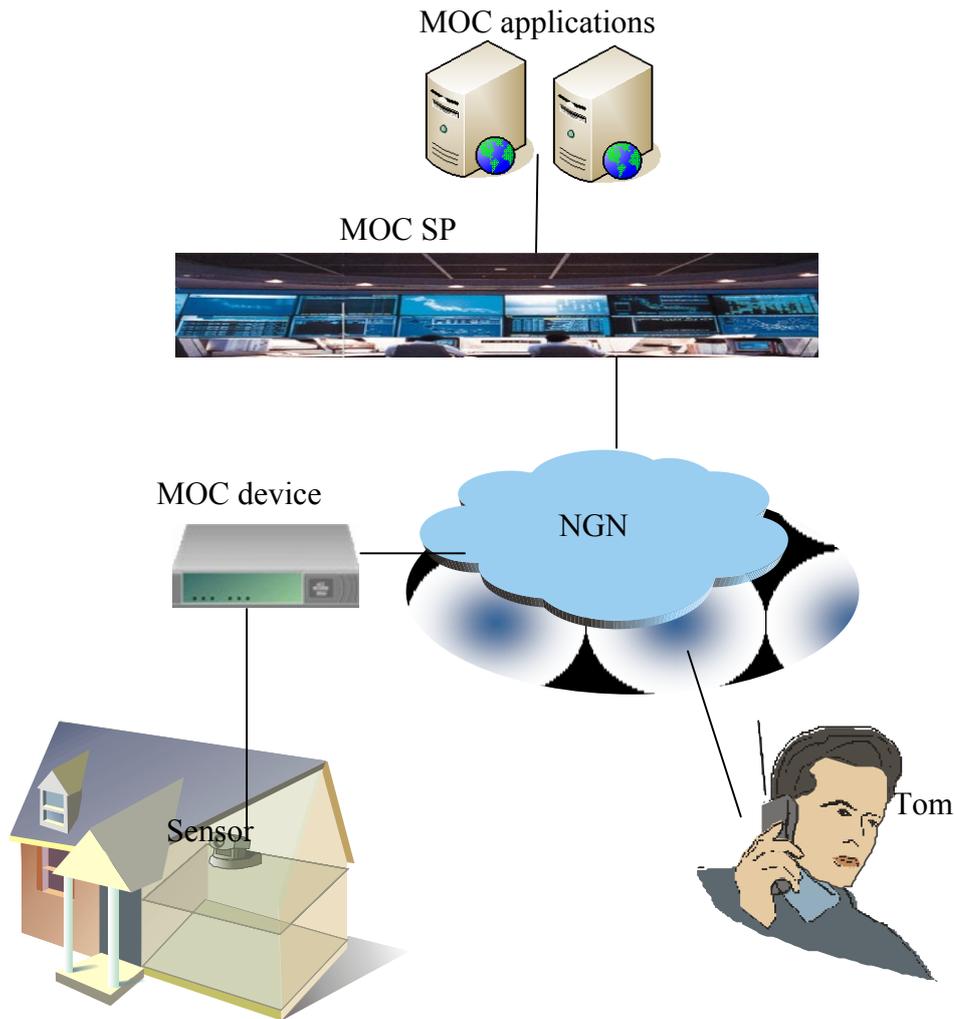


Figure I.4 Communication between machine and human

Editor's note: figure needs to be reviewed to show multiple MOC devices, "MOC device" box should be modified into "MOC gateway".

To support this use case, the following requirements are identified:

- The **MOC SP** can define the policy and send to the MOC device.
- The MOC device executes the policy and detects the sensor to check the conditions defined in the policy.
- The MOC device triggers the executor and/or initiates the conversation defined in the policy.

I.9 Integration with Internet services

Editor's note: 1) the text should be organized with figure and then detailed description associated with the figure. Also, it should be clarified 2) if this use case is related to one or more specific type (types) of communication, 3) the associated requirements similarly to existing use cases in the current draft.

Editor's note: it would useful to describe more the use cases in terms of possible business models (and consequently review the related business models clause in the body).

Editor's note: to review editorial details, to have terminology alignment with the body.

There are many attractive services provided in the Internet, such as SNS, Blog, Twitter, etc., with a huge customer number. MOC can extend the Internet services scope to the MOC ecosystem, and the Internet services can popularize and spread the MOC applications to customers.

The MOC SP provides the functions for the customer to access interested MOC content via the Internet services with defined rules (e.g. publishing times etc.). The MOC SP detects the content and provides it to the Internet services based on the rules. The Internet services then publish the content for customers' browsing or pushing to the customers.

Tom finds that the MOC SP provides real time pictures and videos of city traffic information from the cameras installed in the streets and that information can be provided to subscribers' social network service (SNS). Tom subscribes to this instantaneous traffic update service (e.g. pictures/5-minutes) to receive instantaneous traffic information on his social network service (SNS).

The MOC SP keeps Tom updated via SNS according to Tom's preferences.

Tom can access his SNS to know the highway traffic information on his way to home.

Editor's note: some text is necessary to introduce and describe the figure below.

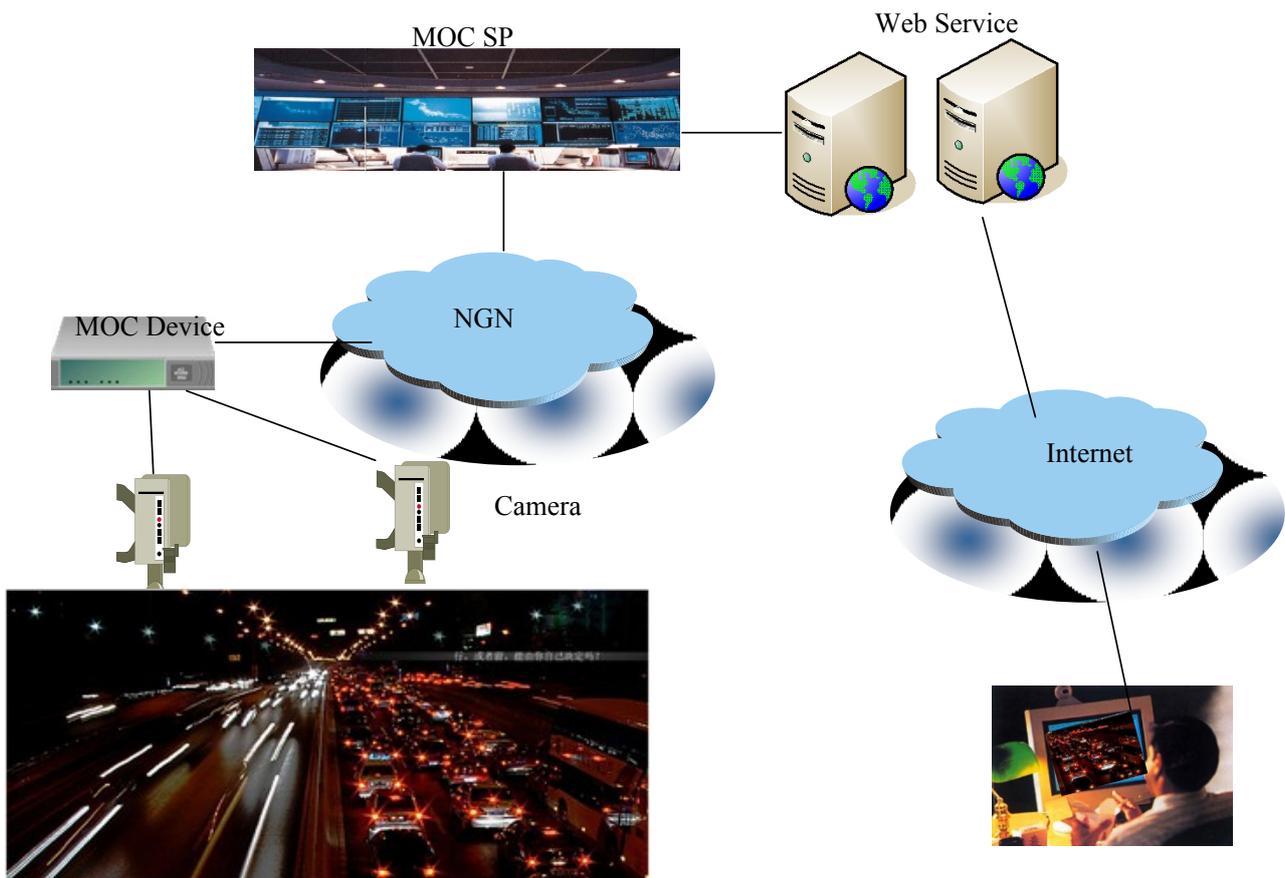


Figure I.5 MOC integration with Internet services

To support this use case, the following requirements are identified:

- A MOC capability is required to enable customers to access relevant MOC content via the Internet services with defined rules.
- A MOC capability is required to detect the relevant MOC content and provide it to the Internet services based on the rules.
- A MOC capability is required to communicate with the Internet services to exchange the information.

Editor's note: "the following text needs to be reviewed and merged/harmonized as appropriate with the above text.

MOC applications integrate with internet services to ensure the customers to use the MOC applications in existing popular Internet services and can extend the value chain and attract more customers.

MOC applications integrate with Internet services using the MOC capabilities. MOC capabilities support setting rules to detect the MOC devices/gateways' data and transfer the data with defined format to the capability which used to communicate with the Internet services for publishing.

- 1) MOC application requires MOC capabilities to support setting rules to detect the MOC devices/ gateways' data and transfer the data with defined format to the capability which used to communicate with the Internet services for publishing.

Appendix II

Gap analysis

(This appendix does not form an integral part of this Recommendation)

Editor's note: The following text has not been reviewed in detail, further review is required.

Table II.1 Gaps analysis between USN and MOC from the service requirements perspective

Requirement	NGN	USN	MOC
Low Mobility	In Paragraph 12 of Y.2201, it specifies the mobility management for NGN. But the mobility in Y.2201 is mainly defined for human-hold devices, such as nomadism, intra-AN, inter-AN, etc. and no description for low mobility management for low human interfered devices, such as MOC devices.	In section 7.2 of Y.2221, it specifies the mobility support for USN sensors, including: 1) a sensor node moving within a sensor network; 2)a sensor node moving across multiple sensor networks; 3)a sensor network moving across infrastructure networks and impacts on infrastructure networks. And there is not mechanism for low mobility in network.	In MOC services, it requires NGN to support low mobility management, such as network optimization for devices that moves rarely or moves within limited area, such as within a cell. Network and network mobility can be simplified accordingly, such as the NodeB, BSC or even base station can handle mobility.
Time controlled	In Y.2201, there is no such kind of description for time control.	There is no such kind of description for time control.	In MOC services, it requires NGN to support time control for MOC devices. The MOC devices can only attach to network and send/receive data packet during the time slot allocated by NGN; otherwise it will be refused to do so. If the attachment to network is out of time, the network should initiate de-attachment.
Low network usage	In Y.2201, there is no such kind of description for time control.	In Y.2221, there is no such kind of description for time control.	MOC services usually involve small amount of data usage or rare network usage, and MOC devices maybe in sleepy mode for most of time, to improve network efficient and decrease the cost of MOC services, both network and communication network needs to be optimized. For example, when the network needs to initiate a service, the network should be able to page on the target device before service interaction.
Inter-working with heterogeneous network	No description	There has description of heterogeneity of nodes, but no description regarding network-side	In MOC services environment, MOC should be able to inter-work with a couple of existing networks to provide more flexible and ubiquitous

Requirement	NGN	USN	MOC
		inter-working between heterogeneous networks.	service experience since there have been deployed various service systems, e.g., Cable TV network, meteorology network, public safety network, banking network, enterprise network, etc. The inter-work may include both transport layer and service layer. For transport layer, it should support mechanism such as trans-code, etc.; for service layer, it should support service adaptation, such as service data format adaptation, etc.
Legacy device access	No description	No description	Since there has been already a lot of legacy MOC devices deployed in market which are not compatible with existing standards, e.g., USN. And MOC system should be able to support such kind of sensors or gateways to access, for example, signalling adaptation, service data adaptation, etc
Service\application collaboration	No description	No description	Since there are many existing service\applications in market which are not quite familiar for customers, and customers can subscribe service to operator or 3 rd party service providers. Hence, operators or 3 rd party service providers should support selecting and correlating target services intelligently for customers, for example, operators should support providing diagnosis between multiple hospitals. When sensors report data to network, the network should support route data to multiple service systems. And multiple service system can jointly co-work for MOC devices.
Location-based Broadcast\Multicast	In Y.2201, NGN can provide broadcast, e.g. group-based, etc.	No description	NGN should support location-based broadcast\multicast, including broadcast to MOC devices within certain target area.
System balance and robustness	In Y.2201, NGN can support communication admission control on a per-NGCN site basis.	No description	MOC devices may distribute variously, and the density of devices in certain area might be high or low and it may cause system imbalance accordingly, in order to support load balance and high availability, NGN network should be enhance to support system balance and

Requirement	NGN	USN	MOC
			robustness.
Multi-gateway	No description in Y.2201	No description	To decrease the load of single MOC gateway or increase the reliability of the access to network, MOC devices can access to network via multiple gateways. And NGN should support multi-gateway access, for example it can identify each device no matter which gateway it connects to, and NGN should also support multiple gateway management, such as attachment or de-attachment.
Group-based billing and charging	No description	There have some kinds of charging and accounting, such as policy-based charging description. But the description is not clear. And there is no description regarding unified charging and group-based charging which is a hot topic in 3GPP MTC WI.	NGN should support group based billing capabilities. When MOC devices under the same group access or communicate with network, the network should charge them as one group, and may not generate different CDR for each single device..

Bibliography

Editor's note: to add all not normative references which are mentioned in the body (e.g. those referred in definitions only such as Y.2240; Q.1703 etc.)

ATTACHMENT: Living list for Y.MOC-Reqts Item 1

From C1054

A.x service convergence of MOC device/gateway and the NGN terminal

Tom and Helen are a husband and wife and living in a smart home with a MOC gateway and some MOC devices in the house which managed by the MOC service provider. One day, Tom is out, Helen and their son Bob are at home, both Helen's NGN terminal and Bob's game machine are connected with the MOC gateway in the home network.

All the MOC devices capabilities are registered in the MOC gateway and those capabilities are recorded and managed by MOC service provider. When Helen's NGN terminal is connected into the home network, Helen can subscribe the MOC capabilities of the terminals in the home network. The MOC gateway can provide the capabilities for Helen's NGN terminal for further use.

Helen can use her NGN terminal to get the MOC devices' data information such as: the temperature in each room, control the light, control the music, and get the alert about the food in the refrigerator is limited, .etc in the home network. Tom also can get that information based on the MOC capabilities by using the NGN network.

Tom uses the NGN terminal to call his wife Helen, in the conversation, Helen wants to show the new style of the house to her husband, she uses the camera's capability in the house for his husband to view the whole house, and Helen can control the direction of the camera for the whole views.

Tom wants to talk with his son at the same time, and his son is play his game machine and the game machine can support the conversation using home network and the capability is provided to Helen's NGN terminal, Helen uses Bob's game machine capability to join the conversation, and Helen can control the session such as: permit/prohibit Tom and Bob's video conference, permit/prohibit Bob's voice with the capabilities, .etc.

1. NGN terminals and Non-NGN terminals can connect with MOC local network.
2. The capabilities of MOC gateway/devices or other terminals should be managed by the MOC gateway or MOC capabilities
3. The capabilities should provide to the terminals wanted.
4. The capabilities can be used which got for NGN conversation for data or media transformation.

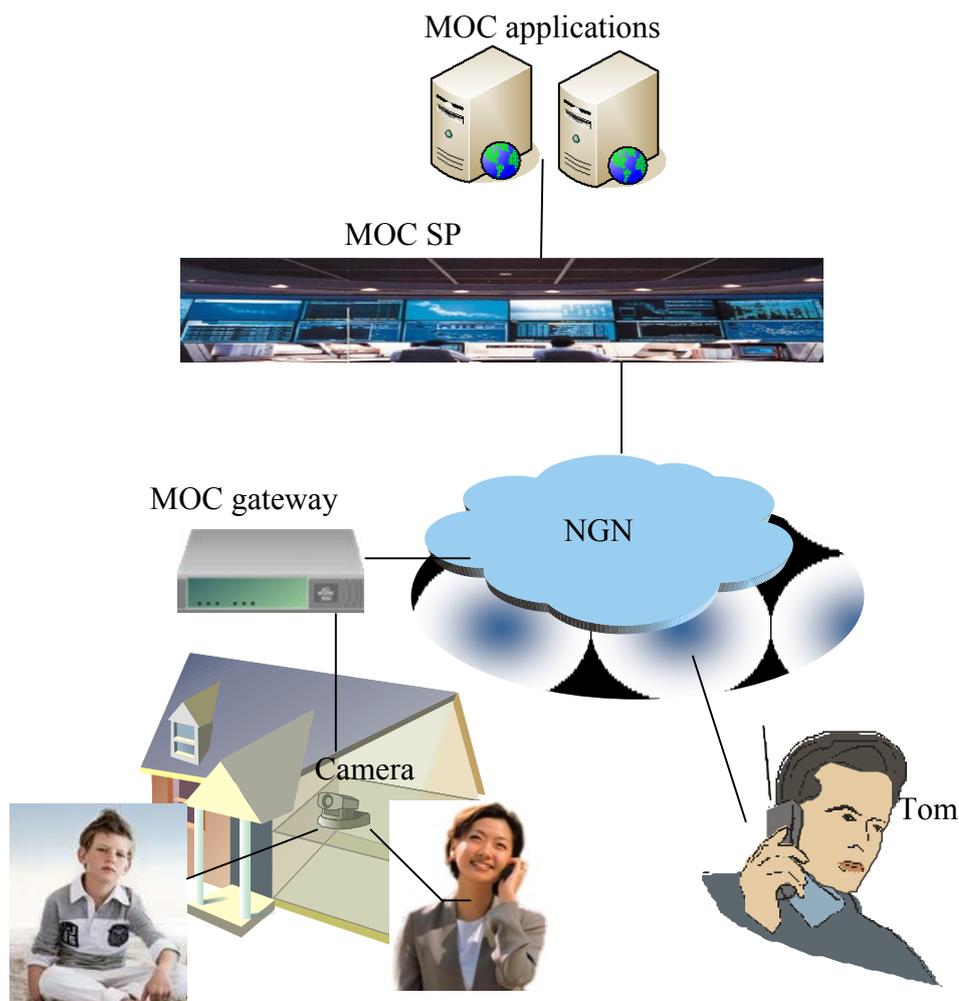


Figure 6-x: service convergence use case

Item 2

From C1053

8 Service requirements of MOC applications

8.x service convergence

MOC application can use the MOC capabilities by standard interfaces, and the capabilities can be converged with existing NGN services.

The MOC gateway and/or MOC capabilities manage the MOC gateway, MOC devices or other devices' capabilities connect with MOC local network and those capabilities can be exposed for MOC applications' development, deployment; those capabilities can also be exposed and converged with NGN terminals with the subscription after authentication in both the local network and the NGN network.

- 1) MOC application can use the capabilities exposed by MOC capabilities or MOC gateway for application's development and deployment.
- 2) MOC application can use the MOC capabilities and converge with existing NGN services.

Item 3

From C965 Relationship between Y.MOC-reqts and Y.SCN

Abstract

This contribution discusses the relationship between SCN and MOC. It proposes to merge the related text of service requirements of the two documents.

Discussion

- **Some definitions are similar.**

In Y.SCN, some terminologies are defined as follows:

Sensor control network is a sensor network intended for managing one or several actuation units. **Mot** is a miniature computing device equipped with sensors (gages for temperature, pressure, illumination, vibration level, location and so on) and signal transceivers operating in a given radio band and used for transmitting sensor readings. A mot can also have the capability to retrieve data on the read-outs of near-site sensors.

actuation unit is an electromechanical device and/or input-output device designed to accomplish certain assignments in the external environment and intended for direct interaction with the external environment through executing different management commands.

“**terminal**”(a device coupled with the actuation unit intended for receiving management commands via the central communications channel, as well as for transmitting to the sever data concerning the status of the actuation unit)

In Y.MOC.reqts, some terminologies are defined as follows:

MOC device: a device with limited or no human intervention involved in the support of MOC applications.

Actuator: a device performing physical actions which has communication capabilities. **MOC**

gateway: A gateway which interconnects MOC local networks and the NGN.

So, “**Mot**” is one type of “**MOC device**”. Functions of “**Acuation unit**” and “**actuator**” are same. Actuation unit connect to NGN though “**terminal**” which is “**MOC gateway**” defined in **Y.MOCreqts**

● **Service requirements are same or similar**

SCN applications exist in:

- everyday life: navigation, excursions, sports;
- medicine: consistent body control, call in an ambulance;
- enterprise: logistics, stock management;
- industrial field: fabrication automation, production process control;
- military field: combat assistance, remote piloting;
- disaster management: early warning, evacuation, orchestration of civilians and rescuers, automatic danger elimination.

These applications are also included in Y.MOCreqts and some use cases are described in appendix I of Y.MOCreqts. Thus, SCN applications and services are one kind of MOC services. Thus, **service requirements of SCN applications should be covered by MOC applications.**

Proposal

1. Move or merge the related text of service requirements of Y. SCN to Y.MOC-reqts.

requirement	proposal
Connectivity	Add new clause in Y.MOC.reqts
Mobility support	Merge into clause 8.1 in Y.MOC.reqts
Context-awareness	Add new clause in Y.MOC.reqts
Routing	Merge into clause 8.11 in Y.MOC.reqts
Load balancing	Merge into clause 8.7 in Y.MOC.reqts
Scalability	Merge into clause 8.10.1
Fault tolerance	Merge into clause 8.10.1
Quality of service (QoS)	Merge into clause 8.14 in Y.MOC.reqts
Management	Merge into clause 8.10 in Y.MOC.reqts
Pledging of security of decisions	Add new clause in Y.MOC.reqts
Open service environment	Add new clause in Y.MOC.reqts
Enhanced service profile management	Merge into clause 8.10 in Y.MOC.reqts
Service convergence	Add new clause in Y.MOC.reqts
Legacy device support	Merge into clause 8.5 in Y.MOC.reqts
Enhanced emergency services	Merge into clause 8.14.2 in Y.MOC.reqts

2. Added related use case of SCN in Y. MOC-reqts
3. Solution aspects of SCN application work item to be treated separately in other documents

Item 4

Comments to C965 from Russian Federation

This input from Russian Federation is intended to clarify the objections against merging of service requirements of SCN and MOC proposed in C.965 and proposes some solutions for that.

NOTE: generally, these comments are also valid with respect to C986.

The main objection is that the proposed version of the document doesn't mention SCN.

There are four ways to provide service requirements for SCN.

1. Replace "MOC" to "MOC and SCN". This is not a good way, because SCN service requirements contain some important points which are not included to this document version.
2. Replace "MOC" to "MOC and SCN" and append the missing requirements from the SCN to final document. This may be a solution but the following problem should be solved:
 - SCN service requirements include some SCN-specific requirements that are generally not applicable to MOC (including, but not limiting to, the fact that MOC doesn't contains some objects such as "mote, mote group, etc", and there the correspondence between MOC and SCN terms wasn't elaborated so far). The list of SCN-specific requirements:
 - A. SCN application is required to support three types of communications:
 - *Server-terminal communication: terminals communicate with the SCN server;*
 - *Infrastructure communication (including one-to-one, one-to-many, many-to-one and many-to-many): motes from different mote groups communicate with each other and with the SCN server;*
 - *Server-external communication: external NGN objects communicate with the SCN server.*
 - ...
 - B. Mobility support includes support of generic objects (i.e. mass mobile devices: phones, notebooks, etc.) which are not generally MOC objects.
 - C. Legacy device support intends providing connectivity with existing mobile devices.
 - D. Service convergence.

The two last points are especially important, because there are already deployed some applications using these features, and a standardization work should be initiated as soon as possible. These items can be a starting point for it.

If these points can be added to the main text, this could be a solution. Otherwise, the following solutions can be discussed:

3. Make a merged text which contains a section with SCN-specific requirements.
4. Keep two separate documents.