

Recommendation ITU-T Y.2061 (ex Y.MOC-Reqs)

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

Summary

This Recommendation provides an overview of machine oriented communication (MOC) applications in the NGN environment, including the description of a MOC ecosystem, characteristics of MOC and some relevant use cases. Analyzing service requirements of MOC applications, it specifies requirements for NGN capabilities and requirements of MOC device domain capabilities based on these service requirements, and then provides a reference framework for MOC capabilities.

Keywords

Machine oriented communication (MOC), MOC applications, MOC capabilities, MOC device, MOC device domain, MOC gateway, MOC service domain, NGN, NGN capabilities, NGN domain, service requirements.

Table of Contents

1	SCOPE	5
2	REFERENCES	5
3	DEFINITIONS	6
3.1	Terms defined elsewhere	6
3.2	Terms defined in this Recommendation	6
4	ABBREVIATIONS AND ACRONYMS	8
5	CONVENTIONS	8
6	INTRODUCTION	9
6.1	Network overview	9
6.2	Types of machine oriented communications	11
6.3	MOC ecosystem	12
7	CHARACTERISTICS OF MOC	14
8	SERVICE REQUIREMENTS OF MOC APPLICATIONS	15
8.1	Mobility levels	15
8.2	Time controlled network communications	16
8.3	Resource usage	16
8.4	Interoperability with proprietary devices	16
8.5	Application collaboration	16
8.6	Support of service integration and delivery environment	17
8.7	Load balancing and robustness	17
8.8	Accounting and charging	17
8.9	Management	18
8.10	Addressing and identification	19
8.11	Location-based support	20
8.12	Group-based support	20
8.13	Quality of Service	21

8.14	Security	21
8.15	Device association and interaction with multiple applications	22
8.16	Communication with sleeping device	23
8.17	Differentiation and handling of collected data	23
9	REQUIREMENTS OF NGN CAPABILITIES	23
9.1	Requirements for extensions or additions to NGN capabilities	23
9.2	Requirements supported by existing NGN capabilities	26
10	CAPABILITY REQUIREMENTS OF MOC DEVICE DOMAIN	27
10.1	Application enablement	27
10.2	Mobility	27
10.3	Communication	27
10.4	QoS	28
10.5	Remote management	28
10.6	Device addressing and identification	28
10.7	Security	29
10.8	Accounting and charging	29
10.9	Data identification	29
11	REFERENCE FRAMEWORK FOR MOC CAPABILITIES	29
11.1	High level view	29
11.2	MOC capabilities in the NGN domain	31
11.3	MOC capabilities in the MOC device domain	33
11.4	MOC service interfaces	34
12	SECURITY CONSIDERATIONS	36
APPENDIX I		37
APPENDIX II		38
II.1	E-Health	38
II.2	Tsunami warning service	40

II.3 Motorcade Management	41
II.4 Smart home	42
II.5 Integration with Internet services	44
BIBLIOGRAPHY	46

Recommendation ITU-T Y.2061 (ex Y.MOC-Reqts)

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

1 Scope

This Recommendation covers extensions and additions to NGN as well as device 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:

- Network overview, description of a MOC ecosystem and characteristics of MOC;
- Service requirements for support of MOC applications;
- Requirements of NGN capabilities based on the MOC service requirements;
- Requirements of MOC device domain capabilities based on the MOC service requirements;
- Reference framework for MOC capabilities.

NOTE – Appendix I provides details about actors and roles in a MOC ecosystem and Appendix II 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 Q.1706] Recommendation ITU-T Q.1706/Y.2801 (2006), *Mobility management requirements for NGN*.
- [ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of the NGN*.
- [ITU-T Y.2060] Recommendation ITU-T Y.2060 (2012), *Overview of Internet of Things*
- [ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN*.
- [ITU-T Y.2221] Recommendation ITU-T Y.2221 (2010), *Requirements for support of Ubiquitous Sensor Network (USN) applications and services in the NGN environment*.
- [ITU-T Y.2233] Recommendation ITU-T Y.2233 (2008), *Requirements and framework allowing accounting and charging capabilities in NGN*.

- [ITU-T Y.2240] Recommendation ITU-T Y.2240 (2011), *Requirements and capabilities for NGN service integration and delivery environment*.
- [ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.
- [ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 device [ITU-T Y.2060]: In the Internet of Things, a piece of equipment with the mandatory capabilities of communication and optional capabilities of sensing, actuating, data capturing, data storing and data processing.

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

3.1.3 ID terminal [b-ITU-T Y.2213]: A device with a data reading and optional writing capability which reads (and optionally writes) identifier(s) and optionally application data from/into an ID tag.

3.1.4 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.

3.1.5 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.

3.1.6 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.

3.1.7 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.

3.1.8 universal IC card (UICC) [b-ITU-T Q.1741.7]: A physically secure device, an IC card (or 'smart card'), that can be inserted and removed from the terminal. It may contain one or more applications. One of the applications may be a USIM.

3.2 Terms defined in this Recommendation

This Recommendation defines or uses the following terms:

3.2.1 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 devices and gateway.

3.2.2 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.

3.2.3 machine oriented communication (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.

3.2.4 machine oriented communication (MOC) capabilities: a set of functions for the support and management of MOC applications, shared by different MOC applications and accessed through a set of standard interfaces.

NOTE 1 - When MOC capabilities are supported by NGN, they provide standard interfaces for MOC applications to MOC devices and gateway for data collection, management and operation. They also reuse or interact with NGN capabilities [ITU-T Y.2201] [ITU-T Y.2240], IT capabilities or Internet capabilities to provide MOC applications.

NOTE 2 - When MOC capabilities are supported by MOC devices and gateway, they interact with NGN functionalities and MOC applications through a set of standard interfaces.

3.2.5 machine oriented communication (MOC) device: A device 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.

3.2.6 machine oriented communication (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).

3.2.7 machine oriented communication (MOC) gateway: A gateway which interconnects and provides interoperability between MOC local networks and the network and where applicable, interoperability at the MOC application level.

NOTE - In the NGN environment, a MOC gateway acts as a proxy or data aggregator to ensure interoperability and interconnection of MOC devices with the NGN.

3.2.8 machine oriented communication (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.

3.2.9 machine oriented communication (MOC) local network: A network which provides connectivity between MOC devices without the intermediation of MOC gateway, and between MOC devices and gateway.

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

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACI	Application to Capability Interface
ANI	Application to Network Interface
API	Application Programming Interface
B2C	Business to Customer
CDR	Charging Data Record
GPS	Global Positioning System
GNSS	Global Navigation Satellite Systems
IC	Integrated Circuit
ID	Identification
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
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
SNS	Social Network Services
UICC	Universal Integrated Circuit Card
UNI	User to Network Interface

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 needs 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) are a form of data communications between two or more entities in which at least one entity does not necessarily require human interaction or intervention in the process of communication.

MOC include communications with remote MOC devices for the support of procedures covering aspects such as registration, authentication, authorization, monitoring, maintenance, provisioning and troubleshooting. MOC applications intend to automate decision and communication processes.

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

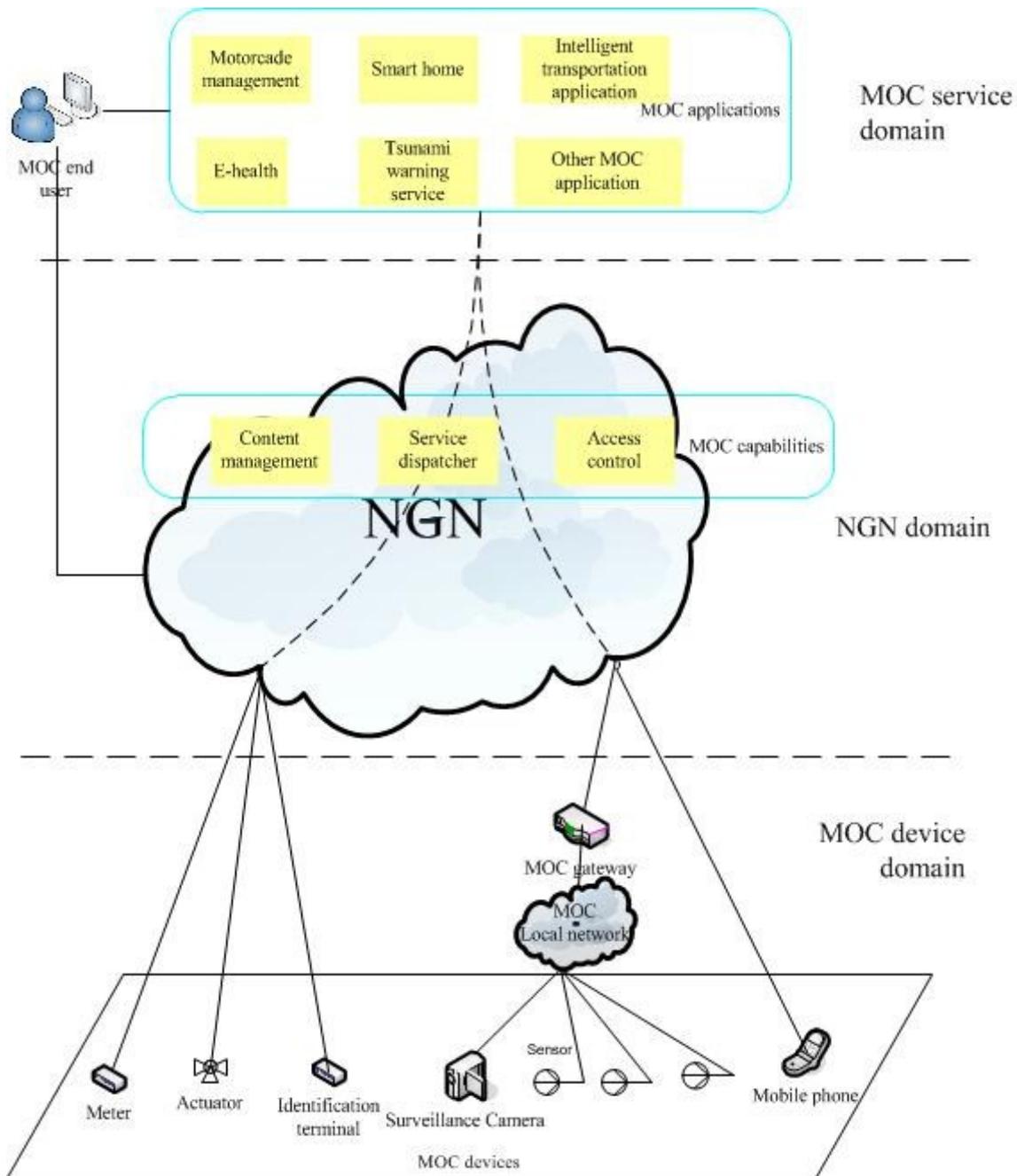


Figure 6-1 - Network overview for support of MOC applications in the NGN environment

The MOC device domain includes MOC devices and MOC gateways. MOC devices include various types of devices as shown in Figure 6-1.

NOTE 1 - Proprietary devices (see Figure 11-1) are not shown in the above figure.

MOC devices can be categorized into general devices, data capturing devices, data carrying devices and sensing or actuating devices [ITU-T Y.2060]. Examples for the different categories include:

- for sensing or actuating devices: sensor, surveillance camera, meter, actuator with remote control;
- for data capturing devices and data carrying devices: Identification terminal (ID terminal);
- for general devices: mobile phone, personal computer, networked television.

MOC devices may access 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 gateway may access NGN via multiple access networks, for example to ensure reliable communications.

The 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 [ITU-T Y.2201], 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 content management, service dispatcher and access control. Details can be found in clause 11.

NOTE 2 – Although not shown in Figure 6-1, MOC capabilities in NGN can also interact with other applications outside the MOC service domain, such as social network services (SNS), Blog applications, which can make available the MOC related information according to the requirements from customers or applications.

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

NOTE 3 – Although not shown in Figure 6-1, MOC capabilities and MOC applications can also exist in the MOC device domain.

6.2 Types of machine oriented communications

MOC covers communications among MOC devices and humans, specifically:

- communications among different MOC devices and among MOC devices and MOC applications;
- communications among MOC devices and other devices controlled by human.

The first type of communications deals with data collection, device management, device operations and other communication functions with remote equipment. These communications are used in many scenarios, e.g. that of MOC applications getting the relevant information provided by sensors.

The second type of communications may be initiated by remote MOC devices to timely inform humans about relevant information detected in MOC devices, or may be initiated by humans to get relevant information from remote MOC devices. These communications involve many scenarios, e.g. that of a human connecting to a surveillance camera in his house by using a mobile phone.

In the case of a MOC device interacting with MOC capabilities in network domain or with MOC applications, the execution of a MOC application 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 physical properties, multimedia data etc.). When the MOC device meets a trigger threshold or receives an instruction from MOC capabilities in network domain or MOC applications, the MOC device requests the NGN to transfer the data to the MOC application;

NOTE 1 - The MOC device follows the pre-configured policy, which can be decided by the MOC capabilities or the MOC applications. According to the policy, the MOC device detects data, executes the logic, and initiates the communication to the MOC applications or

human-controlled MOC devices to report the relevant information.

- 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 (without gateway) under the authorization of MOC capabilities in NGN: in order to manage the MOC device, the MOC application gets the authorization information from the MOC capabilities which are used for secure communication's authorization and session key negotiation;

NOTE 2 - The MOC device may also initiate such process.

- Data analysis: the MOC application analyzes data received from the MOC device. MOC capabilities in NGN 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).

NOTE 3 - Not all of the above phases are necessary for the execution of all MOC applications. For example, a MOC end user can send a request to a vehicle related MOC application to turn on the klaxon of the vehicle when he/she wants to find out his/her vehicle in a large parking area, and the vehicle related MOC application will turn on the vehicle klaxon after receiving the request. In this example, data collection and data transportation from the MOC device (the vehicle) to the MOC application are not executed.

6.3 MOC ecosystem

Figure 6-2 depicts business roles which are relevant in a MOC ecosystem, and their relationships.

The business roles identified in Figure 6-2 and their relationships are based on the IoT ecosystem [ITU-T Y.2060] and adapted to the context of MOC.

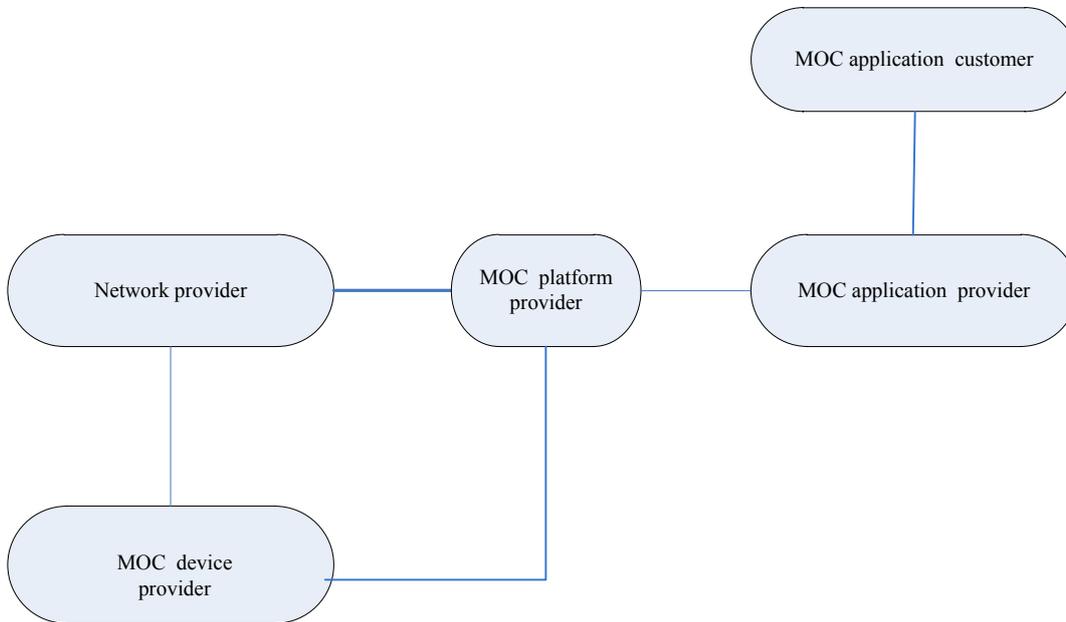


Figure 6-2 - Business roles in a MOC ecosystem

Five key roles are identified: MOC application customer, network provider, MOC device provider, MOC platform provider and MOC application provider.

- Network provider

In the context of this Recommendation, the network provider is the role that offers the NGN capabilities as described in [ITU-T Y.2201].

The network provider has business relationship with the MOC platform provider and the MOC device providers.

NOTE 1 - An actor playing the role of network provider can also play the roles of MOC platform provider, MOC device provider and MOC application provider.

- MOC application provider

The MOC application provider is the role providing functions in the MOC service domain. It utilizes capabilities provided by the MOC platform provider in order to provide services to the MOC application customer.

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

NOTE 2 - An actor playing the role of MOC application provider can also play the role of MOC platform provider.

- MOC device provider

The MOC device provider is responsible for providing functions in the MOC device domain. It provides raw data or other necessary resources to the network provider and the MOC platform provider according to the service logic.

The MOC device provider has business relationship with the MOC platform provider and the network provider.

NOTE 3 - An actor playing the role of MOC device provider can also play the role of MOC application provider and the MOC platform provider.

- MOC platform provider

The MOC platform provider is the role responsible for providing the following functions in the NGN domain:

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

The MOC platform provider has business relationship with the MOC device provider, the MOC application provider and the network provider.

NOTE 4 - An actor playing the role of MOC platform provider can also play the role of MOC application provider and MOC device provider.

- MOC application customer

The MOC application customer may be a human or a device. The MOC application customer consumes applications offered by the MOC application provider. Organizations or persons such as enterprise, family, individual are examples of MOC application customers.

The MOC application customer has business relationship with the MOC application provider. The MOC application customer is a subscriber of the MOC application provider.

NOTE 5 - A given MOC application customer can represent multiple MOC end-users in the MOC service domain.

Appendix I provides details about actors and roles in the MOC ecosystem.

7 Characteristics of MOC

This clause provides characteristics of MOC including for applications, devices and gateways. Consideration should be given to the fact that these characteristics may vary across MOC applications, devices and gateways. These characteristics include, but are not limited to, the following ones:

- 1) Variety of MOC device types and capability levels

There are various types of MOC devices for different usage, some of them having low performance and limited functionality (e.g. low processing capability, small memory, limited security capabilities), others having powerful embedded capabilities (e.g. bilateral authentication and authorization capabilities with the network and MOC applications).

- 2) MOC applications support of heterogeneous MOC devices

MOC applications may communicate with more than one type of MOC devices. In such cases, MOC applications need to cope with this heterogeneity.

3) Grouping of MOC devices

In some use cases, groups of MOC devices are deployed for services. Usually, the MOC devices of a specific group have the same characteristics, functions, performance or policies.

4) Variety of mobility levels of MOC devices and gateway

Some MOC devices and gateway are mobile everywhere. Some of devices and gateway do not move. Some MOC devices and gateway move only within a certain area. Some MOC devices and gateway should not move after installed (their movement would mean theft of these devices).

5) Remote management of MOC devices in varied and large deployments

Because massively deployed MOC devices cover large areas, exist for a long time and may be moving, it is difficult for operators or MOC end user to manage in the field all devices.

Remote management functionality of MOC devices (e.g. firmware update) is particularly important in such deployments.

6) Increased security threats from limited manual intervention

Some MOC devices and gateway are required to be managed remotely rather than operated manually infield. This increases the security threat level, such as physical tampering, hacking, and unauthorized monitoring and so on. So adequate security measures should be provided to detect or resist possible attacks.

7) Variety of data communication characteristics

Most of MOC applications depend on data communications driven by machines without human interventions. The characteristics of such data communications are much different from human driven communications.

The variety of data communications is also caused by the variability of other factors, such packet size (small or large packets), data transmission period and frequency, MOC device communication role (initiating party or terminating party).

8) Large amount of data transmitted to the network

With more and more intelligence embedded in devices and the large number of devices connected to the network, large amounts of data are transmitted to the network.

8 Service requirements of MOC applications

8.1 Mobility levels

Different types of MOC applications may require different levels of MOC device and/or gateway mobility. This includes no mobility for devices and gateway that do not move, limited mobility for devices and gateway that move infrequently (e.g., medical devices on a patient may not move frequently), or low geographical mobility for devices and gateway that move only within a certain region (e.g., bus equipment devices such as a camera may move only within a city). It is needed to provide mobility management for different mobility levels in order to reduce resource usage (e.g. the timer of periodic location update should be reduced for the MOC devices which have infrequent movement).

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.

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.

Requirements for time controlled network communications are as follows:

- 1) MOC applications are recommended to support time control for MOC device communications with the network based on service criteria (e.g. daily network traffic load, MOC device location).

8.3 Resource usage

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

MOC applications requirements for optimized resource usage are as follows:

- 1) MOC applications are recommended to optimize the usage of resources of both MOC devices and network.

NOTE - This is particularly relevant in case of infrequent data transmissions.

8.4 Interoperability with proprietary devices

Since a lot of proprietary devices (e.g., devices with proprietary standards for inter-working with network entities) have already been deployed, MOC applications should be able to support interoperability with these proprietary devices.

Requirements for support of proprietary devices are as follows:

- 1) It is recommended that MOC applications be interoperable with proprietary devices through appropriate means, e.g. MOC gateways;
- 2) MOC applications are recommended to support the effective hiding of proprietary devices' operations.

8.5 Application collaboration

For some MOC applications cases, there may be multiple MOC application providers providing different MOC applications which need to collaborate between each other.

As an example, business to customer (B2C) companies deliver products to logistics companies for further delivering to the customers who have ordered them. Logistics companies track the products in transit, while customers may check the whereabouts of the purchased products by visiting the application systems of the B2C companies which collaborate with the application systems of the logistics companies.

MOC applications requirements for application collaboration are as follows:

- 1) MOC applications are recommended to support application collaboration with other MOC applications via the intermediation of the MOC capabilities;

- 2) MOC applications of a given MOC application provider are recommended to support of application collaboration with MOC applications of other MOC application providers via the intermediation of the MOC capabilities.

8.6 Support of service integration and delivery environment

MOC applications would benefit from support by the network of a service integration and delivery environment. In addition to the support of common purpose capabilities for different types of applications, interfaces to such environment would enable support of specific capabilities for MOC applications.

MOC applications requirements for support of service integration and delivery environment are as follows:

- 1) MOC applications are recommended to be able to access service integration and delivery environment capabilities provided by the network.

NOTE - Access to such an environment also provides access to application development and testing capabilities.

8.7 Load balancing and robustness

In some application cases, e.g. in a river control application with the water level of the river reaching the alert threshold, a large number of monitor points may send alert information to the MOC capabilities in NGN domain, including the possibility to send real-time video. Such emergency scenarios require robustness of the network and MOC capabilities in NGN domain.

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 imbalance in the network and MOC capabilities in NGN domain for both signalling and data traffic.

In order to support network and MOC platform load balancing and robustness, the requirements are as follows:

- 1) MOC applications require mechanisms in the network and MOC capabilities in NGN domain for load balancing;
- 2) MOC applications require robustness of network and MOC capabilities in NGN domain, including ensuring a sufficient level of QoS under given circumstances, e.g. emergency scenarios.

8.8 Accounting and charging

Different charging and accounting requirements need to 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 may be based on the number of communications. Some other MOC applications may rarely connect to the network but generate large amounts of data for each communication, in this case charging and accounting may be based on the amount of data. In other cases, charging and accounting may be based on the duration of communications.

As a MOC application may use multiple devices for a single customer, charging per each device by MOC application providers or network providers would generate a lot of charging data records (CDR) that impose heavy load to some functions, e.g. the charging function. 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 are required to support different charging and accounting methods, such as charging based on the duration of communications, number of communications, amount of transmitted data, etc;
- 2) MOC applications are recommended to support unified charging for customers;
- 3) When group-based support is enabled (see clause 8.12), MOC applications are required to support on-line and off-line accounting and charging based on groupings.

8.9 Management

8.9.1 Device management

MOC devices cover a large area, exist for a long time and could be moving, so it may be difficult for operators or subscribers to manage these devices manually. Thus, MOC devices and gateway should be managed and monitor remotely (for example, updating the firmware to correct faults).

MOC devices with universal integrated circuit card (UICC) may be deployed outdoor without human supervision and it might happen that a given UICC is put into another device without permission of the UICC owner. Thus, in order to avoid such issues, the change of association between MOC device and UICC should be accessible by MOC applications interacting with those MOC devices.

When MOC devices and gateway provide service logic, the MOC devices and gateway provide support capabilities for both the customer and the service. MOC devices and gateway are required to be managed in terms of both network and service management.

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 gateway for various aspects, including:
 - a) abnormal behaviour of MOC devices and gateway, such as acting service not aligned with the subscribed feature;
 - b) the association between the MOC devices and gateway and the UICC;
 - c) the attachment information of MOC devices and gateway, such as attachment location;
 - d) the connectivity of MOC devices and gateway.
- 3) MOC applications are required to support mechanisms to perform simple and scalable pre-provisioning of MOC devices and gateway, enable and disable features, report errors from devices, query about device 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 devices and/or 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

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, MOC application provider identifier and application data types.

MOC applications have the following requirements:

- 1) MOC applications are recommended to use standard service profiles for 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 MOC devices and MOC gateway. As there are various types of MOC devices and MOC gateways, the device profiles are helpful in the management of large numbers of heterogeneous devices and gateways.

NOTE 1 - The MOC device profile information may include MOC device identifier, MOC device type, MOC device capabilities and MOC device location.

MOC applications have the following requirements:

- 1) MOC applications are recommended to use and manage standard device profiles for MOC devices and gateway, including their registration and discovery.

NOTE 2 - Device profile management includes the creation of associations between MOC devices (gateways) and service profiles.

8.10 Addressing and identification

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 multiple gateways scenario allows the reduction of MOC gateways' load and the growth of 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 network via MOC gateways. MOC application servers and MOC 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 to be able to operate with different types of MOC device addressing schemes, e.g. IP addressing and non-IP addressing schemes;
- 2) MOC applications require support of unique identification of MOC devices;
- 3) MOC applications require support of unique identification of MOC groups (see clause 8.12 for description of MOC group);
- 4) MOC applications require support of addressing mechanisms enabling communication with MOC devices behind a MOC gateway;
- 5) MOC applications require support of addressing mechanisms enabling communication with MOC gateways;
- 6) MOC applications require support of unique identification of MOC gateways.

8.11 Location-based support

Location data may be collected by the MOC applications from MOC devices and gateway or from the network. Types of location information include global navigation satellite systems (GNSS), latitude or longitude data or cell identifier (CellID).

MOC applications have the following requirements:

- 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 or multicast method;
- 2) MOC applications are recommended to maintain and manage location information of both a single MOC device and a set of MOC devices behind a MOC gateway;
- 3) MOC applications are recommended 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.

MOC applications may have static MOC groups which are pre-configured, for example the consumer could pre-configure the MOC devices 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.

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

The requirements for group-based support are the following:

- 1) MOC applications require support of static and dynamic MOC groups;
- 2) MOC applications require support of data transmission to/from one or all members in a MOC group using group identifier;
- 3) MOC applications require support of group based QoS policy;
- 4) MOC applications require support of group based traffic parameters;
- 5) MOC applications require support of MOC group management, including display/creation/modification/deletion of MOC groups and associated attributes and display/addition/modification/deletion of MOC group members;
- 6) MOC applications are recommended to be able to send data per MOC group, and apply data prioritization according to member's data prioritization in the MOC group.

8.13 Quality of Service

8.13.1 Application traffic control

The application traffic is not only generated by the MOC devices, but also generated by the MOC applications.

MOC applications often cover a large number of MOC devices and gateways. In such scenarios, from the viewpoint of applications, their QoS may be impacted by high application traffic.

From the viewpoint of the network, the QoS of MOC applications may be improved if the application traffic is well managed.

MOC applications have the following requirements:

- 1) MOC applications require mechanisms for application traffic management, e.g. to limit the maximum number of application transactions per second;
- 2) MOC applications require that access concentration into a single resource is avoided.

8.13.2 Data prioritization

The MOC mission-critical applications 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. In order to provide alarm notification, the emergency data are carried over the network.

MOC applications have the following requirements:

- 1) MOC applications are recommended to be able to set the prioritization of data (within a single application or among different applications);
- 2) MOC applications are recommended to be able to manage different data according to their prioritization;
- 3) MOC applications are recommended to be able to apply data prioritization to MOC devices and gateways according to the related service level agreements (SLA) between MOC application customers and MOC application provider.

8.14 Security

8.14.1 Authentication and authorization

The MOC end users accessing the MOC applications need to be authenticated and authorized. Access to applications has to align with the relevant security levels.

The MOC devices involved in the MOC applications and directly connected need to be authenticated and authorized.

The MOC devices involved in the MOC applications and connected via a MOC gateway should generally be authenticated and authorized.

Requirements of authentication and authorization are as follows:

- 1) MOC applications are required to support authentication and authorization of MOC end users to access MOC applications and related data according to the related security levels;
- 2) MOC applications are required to support a mechanism for authentication and authorization of directly connected MOC devices associated with the MOC applications themselves;
- 3) MOC applications are recommended to support a mechanism for authentication and authorization of MOC devices which are in a MOC local network (connected via a MOC

gateway) and which are associated with the MOC applications themselves;

- 4) MOC applications are required to support a mechanism for registration of directly connected MOC devices associated with the MOC applications themselves.

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 the security view point.

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 the MOC devices roam from one network domain to another network domain;
- 2) MOC applications are required to support integrity and confidentiality of the data exchanged during the application operations;
- 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 are required to be unknown to unauthorized entities. For example, private or sensitive data of a MOC device should not be sent to an unauthenticated end user if this end user initiates a communication with that MOC device.

Due to the limited capabilities of the MOC devices with no support of authentication and authorization functionalities, MOC applications have the following requirements:

- 1) Before MOC device resources can be used by MOC end users and MOC applications, MOC applications are required to support mechanisms for authentication and authorization of MOC end users and MOC applications for their access to MOC device resources.

8.15 Device association and 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 not prevent delivery of information to other MOC applications by a MOC device or gateway associated with that MOC application;
- 2) MOC applications are required to not prevent a MOC device or gateway associated with that MOC application to receive information from other MOC applications.

NOTE - In this Recommendation, it is assumed that the capability of a MOC device or gateway to communicate with multiple applications is controlled by the network (i.e. NGN). Requirements on a MOC device or gateway with network control independent capability to communicate with multiple applications are for further study.

8.16 Communication with sleeping device

In case of offline status for a given period of time, MOC devices enter or 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 being 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 are recommended to be able to send instructions to a sleeping MOC device to wake it up;
- 2) MOC applications are required to support network-initiated communications towards a sleeping MOC device.

8.17 Differentiation and handling of collected data

With the large variety of data collected by MOC devices being transmitted in the network, it is expected that the network be able to differentiate the particular collected data from other data, and then trigger the relevant processes based on their category. For example, the network may cache and forward only later data which are collected in non-network performance sensitive applications. On the other hand, the network is required to transmit immediately high priority data which are collected in network performance sensitive applications.

MOC applications requirements for collected data differentiation and related handling are as follows:

- 1) MOC applications are required to enable identification and categorization of the data collected by MOC devices according to relevant policies;
- 2) If the network can handle data collected by MOC devices according to relevant data categorization, MOC applications are required to manage these data accordingly.

9 Requirements of NGN capabilities

9.1 Requirements for extensions or additions to NGN capabilities

This clause identifies extensions or additions to NGN capabilities defined in [ITU-T Y.2201] for support of MOC applications.

9.1.1 Numbering, naming and addressing

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

Based on the service requirements in clause 8.12, NGN is required to support the following additional numbering, naming and addressing requirements.

- 1) NGN is required to provide group based addressing mechanisms for the support of MOC applications according to the NGN provider's policy;
- 2) NGN is required to support static MOC grouping capability;

NOTE 1 - A static MOC group contains the members of MOC devices and gateway which are pre-configured.

- 3) NGN is required to support dynamic MOC grouping capability;

NOTE 2 - A dynamic MOC group may be generated upon request using specific criteria, such as location, status of MOC devices and gateway, etc.

- 4) NGN is required to support MOC grouping capability in both cases of groups constituted by MOC devices and gateway directly or indirectly connected to NGN;
- 5) NGN is required to map the MOC group identifier to network addresses of MOC devices and gateway of a static MOC group;
- 6) NGN is required to identify the list of MOC devices and gateway and their network addresses matching the specified criteria for dynamic MOC group.

9.1.2 Quality of service

The differentiated quality of service and data prioritization requirements specified in clause 8.13 are supported by the existing capabilities of NGN [ITU-T Y.2201] [ITU-T Y.2221]. The following sub-clauses identify requirements for extensions to NGN.

9.1.2.1 Per group QoS policy

Based on the service requirements in clause 8.12, the following additional requirements are placed on NGN:

- 1) NGN is required to support per group level QoS policy, in parallel to, or instead of, per device level QoS policy.

NOTE - 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

NGN provides processing and traffic management capabilities. The service requirements specified in clause 8.7 are supported by the existing capabilities of NGN [ITU-T Y.2201].

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. attachment to the network or establishment of a data connection) during a defined granted network communication access time interval;
- 2) NGN is required to reject MOC end users' access (e.g. attachment to the network or establishment of 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 and gateway;

- 5) NGN is required to terminate MOC end users' access (e.g. detachment from the network or release 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 and gateway (e.g. MOC application server).

Based on resource usage requirements in clause 8.3 and 8.16, the following additional requirements are placed on NGN:

- 7) NGN is required to page on the target MOC devices and gateway before service interaction when the network needs to initiate a service;
- 8) NGN is required to establish communication resources only when data transmission is required.

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

- 9) Optimized handling of group communications in order to save network resources and to prevent network congestions;
- 10) Per group level traffic control in parallel to, or instead of, per device level traffic control.

NOTE - 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 8.8, the following additional requirements are placed on NGN [ITU-T Y.2233]:

- 1) 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

NGN provides mobility support for end users, MOC devices and gateways [ITU-T Y.2201] [ITU-T Q.1706].

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

- 1) NGN is required to support pre-defined mobility levels for MOC devices and gateway via device profile management;
- 2) NGN is required to support different mobility level management according to the mobility requirements of MOC devices and gateway, such as reducing the frequency of the mobility management procedures for MOC devices and MOC gateway with low mobility;
- 3) NGN is recommended to support dynamical instruction of the MOC devices and gateway in order to set the mobility level (implying, for example, the adjustment of the frequency of the mobility management procedures).

9.1.5 Profile management

9.1.5.1 User profile management

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

- 1) NGN is recommended to support standard service profiles with enhancements for MOC applications' specific information.

9.1.5.2 Device profile management

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

- 1) NGN is recommended to support standard device profiles with enhancements for MOC devices and gateway's specific information.

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 manage and control MOC devices and gateways, including:
 - a) monitoring of MOC devices and gateway's operations;
 - b) where applicable, monitoring of changes, and related actions, in the associations between MOC devices or gateway and UICCs;
 - c) monitoring of changes, and related actions, related to the network attachment points of MOC devices and gateway;
 - d) monitoring of MOC devices and gateway's network connectivity.

9.1.7 Data differentiation and handling

Based on the requirements of differentiation and handling of collected data in clause 8.17, the following additional requirements are placed on NGN:

- 1) NGN is recommended to be able to identify data according to relevant categories;
- 2) NGN is recommended to apply different data handling (e.g. caching and/or forwarding) based on data identification.

9.1.8 Application collaboration and environment for service integration and delivery

Based on the service requirements specified in clauses 8.5 and 8.6, the following additional requirements are placed on NGN:

- 1) NGN is required to provide capabilities for application collaboration and for service integration and delivery environment.

NOTE – [ITU-T Y.2240] capabilities may be used for support of such requirements.

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 for support of MOC applications.

9.2.1 Group management

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

9.2.2 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 capabilities of NGN [ITU-T Y.2201].

9.2.3 Security

NGN provides security capabilities. The service requirements specified in clause 8.13 are supported by the existing capabilities of NGN [ITU-T Y.2201] [ITU-T Y.2701].

9.2.4 Group related communication modes

Based on the service requirements in clause 8.12, NGN is required to support the following communication modes for MOC groups (with MOC devices and gateway directly or indirectly connected to NGN):

- anycast;
- multicast;
- broadcast.

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

10 Capability requirements of MOC device domain

This clause identifies the capability requirements of MOC device domain for the support of MOC applications.

10.1 Application enablement

Based on the requirements in clause 8.4, the following requirements apply to the MOC gateway and MOC device's capabilities:

- 1) MOC devices are recommended to support a set of abstracted operations;
- 2) MOC devices are recommended to support the implementation of service logic to provide MOC capabilities;
- 3) MOC gateways can optionally support a set of abstracted operations on MOC devices;
- 4) MOC gateways can optionally 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's capabilities:

- 1) MOC gateways 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 and 8.4, the following requirements apply to the MOC gateway and MOC device's capabilities:

- 1) MOC gateways and MOC devices are required to be able to establish, maintain or release communication resources according to the data communication needs;
- 2) MOC gateways are required to be able to select the proper routing paths between the traffic originating endpoint (MOC devices or MOC application server) and the traffic receiving endpoint (MOC devices or MOC application server) according to the application the MOC device is associated with or vice versa;

- 3) MOC gateways are required to allow setting and modification of granted/forbidden network communication access time schedules and durations;
- 4) MOC gateways are required to support the following communication modes according to the service requirements:
 - anycast;
 - multicast;
 - broadcast.
- 5) MOC gateways are recommended to support communication with proprietary devices (e.g., devices with proprietary interfaces for inter-working with network entities);
- 6) MOC devices are required to go offline when no data transmission is required, and then to go in sleeping mode according to policies;

NOTE - It is for further study if the transition to sleeping mode can be also controlled by the network.
- 7) MOC devices can optionally support communication with the network according to the following criteria: daily network traffic load, MOC device location, access time schedules and durations.

10.4 QoS

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

- 1) MOC gateways and MOC devices are required to support the traffic control policy which defines granted network communication access time schedules and durations;
- 2) MOC gateways and MOC devices are required to support QoS differentiation according to different categories of traffic;
- 3) MOC gateways and MOC devices are required to provide performance measurement and management;
- 4) MOC gateways and MOC devices are recommended to support application prioritization.

10.5 Remote management

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

- 1) MOC gateways are required to act as a management proxy for MOC devices of the connected MOC local network. This includes support of management requests from NGN and local (to the MOC local network) firmware and software management;
- 2) MOC devices are required to support software and firmware management;
- 3) MOC gateways and MOC devices are required to support configuration management;
- 4) MOC gateways are required to support fault and performance data collection and storage;
- 5) MOC devices are recommended to support fault and performance data collection and storage.

10.6 Device addressing and identification

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

- 1) MOC gateways are required to support mapping between the identification of a MOC device and one or more MOC local network addresses;

- 2) MOC gateways are required to support mapping between the identification of a MOC device group and one or more MOC local network addresses for each MOC device within the group;
- 3) MOC devices are required to support unique identification within the context of a single MOC application;
- 4) A MOC gateway can optionally use temporary identifiers for MOC devices connecting and disconnecting to the network dynamically;
- 5) A MOC gateways can optionally re-assign dynamically released temporary identifiers to other MOC devices.

10.7 Security

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

- 1) MOC gateways are required to identify and authenticate MOC applications, other MOC devices and MOC end users;
- 2) MOC gateways are required to support mechanisms for secure transport, such as encryption and integrity protection;
- 3) MOC devices are recommended to identify and authenticate MOC applications, other MOC devices and MOC end users;
- 4) MOC devices are recommended to support mechanisms for secure transport, such as encryption and integrity protection.

10.8 Accounting and charging

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

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

10.9 Data identification

Based on the requirements of collected data differentiation and related data handling in clause 8.17, the following requirements apply to the MOC device and MOC gateway's capabilities:

- 1) MOC gateways are recommended to make data identifiable according to relevant policies;
- 2) MOC devices can optionally make data identifiable according to relevant policies.

11 Reference framework for MOC capabilities

11.1 High level view

Figure 11-1 provides a high level view of the reference framework for MOC capabilities.

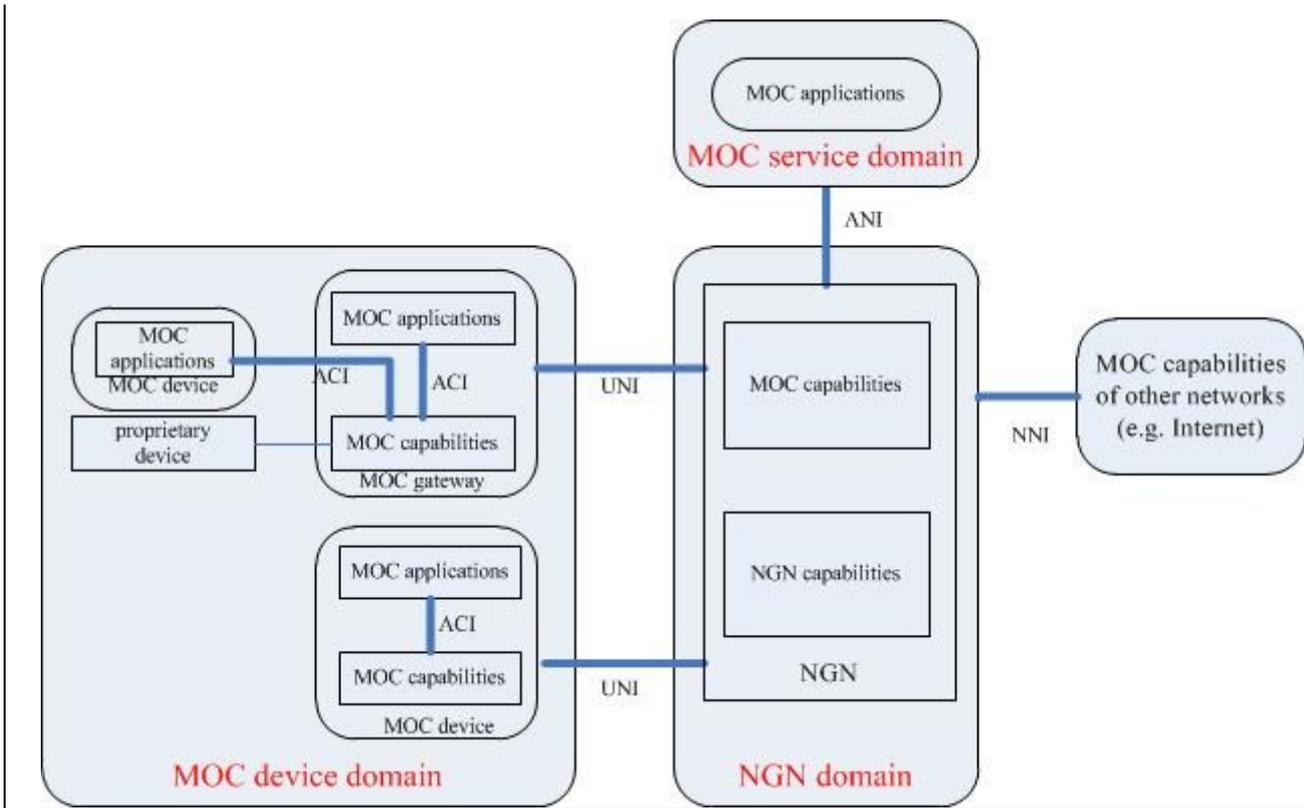


Figure 11-1 - High level view of the reference framework for MOC capabilities

The MOC device domain is composed of MOC devices, proprietary 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 interface between MOC devices or gateways and the NGN is the user to network interface (UNI).

The interface between MOC capabilities and MOC applications residing in the MOC device domain is the application to capability interface (ACI).

The NGN domain is composed of:

- NGN capabilities (modified and extended as necessary for the support of MOC applications as per clause 9);
- MOC capabilities.

The interface between the NGN and other networks is the network to network interface (NNI).

The MOC service domain is composed of MOC applications.

The interface between the NGN and MOC applications residing in the MOC service domain is the application to network interface (ANI).

In order to support MOC applications, service interfaces are provided across ACI, ANI, NNI and UNI. The requirements of these service interfaces are given in clause 11.4.

11.2 MOC capabilities in the NGN domain

The main MOC capabilities in the NGN domain are shown in Figure 11-2. These capabilities provide standard interfaces for MOC applications to MOC devices and gateway for data collection, management and operations.

The MOC capabilities shown in Figure 11-2 are [ITU-T Y.2240] capabilities adapted as necessary to the context of MOC.

In line with [ITU-T Y.2240], the MOC capabilities also interact with NGN capabilities [ITU-T Y.2201], IT capabilities or Internet capabilities.

NOTE 1 - The MOC capabilities in the NGN domain are positioned inside the NGN service stratum [ITU-T Y.2012].

NOTE 2 – Other [ITU-T Y.2240] capabilities are not precluded to be part of, or adapted as, MOC capabilities in the NGN domain as shown in Figure 11-2.



Figure 11-2 - MOC capabilities in the NGN domain

11.2.1 Accounting and charging

This capability supports accounting and charging modes and mechanisms for MOC applications, including:

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

For further details on this capability see [ITU-T Y.2240].

11.2.2 Access control

This 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 application programming interfaces (APIs) and protocols across different service interfaces as well as access from applications to functionalities exposed by MOC capabilities.

For further details on this capability see [ITU-T Y.2240].

11.2.3 Service dispatcher

This capability provides unified message routing and message exchange mechanisms among the MOC capabilities in NGN domain.

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

For further details on this capability see [ITU-T Y.2240].

11.2.4 Content management

Content can be provided as resources to MOC application or end users by different MOC device 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 capabilities in NGN domain 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 MOC applications, content for specific MOC end user.

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

For further details on this capability see [ITU-T Y.2240].

11.2.5 Application provisioning

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

For further details on this capability see [ITU-T Y.2240].

11.2.6 Context management

This 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.

For further details on this capability see [ITU-T Y.2240].

11.2.7 MOC resource registry

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

This capability defines a mechanism for a resource of a MOC device provider to be registered within the MOC capabilities in NGN domain, so that this resource can be located and accessed by applications.

This capability corresponds functionally to the resource registry capability in [ITU-T Y.2240] when adapted to the context of MOC.

11.2.8 MOC resource repository

This capability provides functionalities for the storage of information related to the registered MOC resources. Being stored 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 for application developers.

This capability corresponds functionally to the resource registry capability in [ITU-T Y.2240] when adapted to the context of MOC.

11.2.9 MOC resource manager

This capability performs the control functions for resources provided by NGN and MOC devices in order to satisfy the MOC applications' requirements, including management of the dynamic information concerning the reachability status of MOC devices (e.g. online/offline, forwarding information).

This capability corresponds functionally to the resource registry capability in [ITU-T Y.2240] when adapted to the context of MOC.

11.3 MOC capabilities in the MOC device domain

The MOC capabilities in the MOC device domain are shown in Figure 11-3.

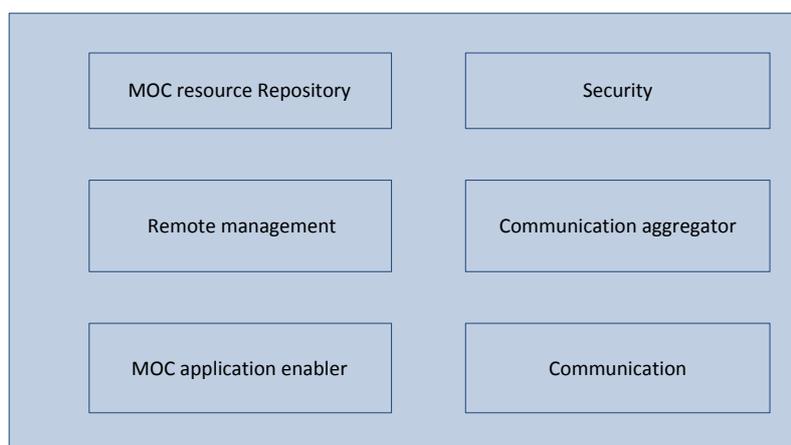


Figure 11-3 - MOC capabilities in the MOC device domain

11.3.1 Communication aggregator

This capability, residing in MOC gateways, performs proxy and traffic aggregator functions.

Based on the requirements identified in clause 10.3, the communication aggregator capability supports relaying of traffic between MOC devices and NGN, QoS mechanisms based on MOC application policy, recording of charging information for MOC devices within the MOC local network

11.3.2 MOC application enabler

Based on the requirements identified in clause 10.1, this capability performs the exposure to MOC applications of MOC capabilities residing in MOC gateway and MOC devices.

11.3.3 MOC resource repository

Based on the requirements identified in clause 10.1, this capability, residing in MOC gateways, provides functionalities for the storage of information related to the registered MOC devices. Being stored in the MOC device repository, the MOC devices' data can be read by the authenticated and authorized MOC applications.

11.3.4 Remote management

Based on the requirements identified in clause 10.5, this capability supports configuration management, fault management, performance management, software and firmware upgrade of MOC gateway and MOC devices in the MOC local network.

NOTE - The functions above can also be realized by local management capabilities of the MOC devices and gateway.

11.3.5 Security

Based on the requirements identified in clause 10.7, this capability performs registration and mutual authentication with MOC applications.

The security capability provides encryption and integrity protection on data exchanged with the NGN and MOC applications to ensure secure delivery.

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

11.3.6 Communication

Based on the requirements identified in clauses 10.3, 10.6, 10.8 and 10.9, this capability performs the generic communication functions in MOC devices and gateway.

The communication capability provides application data transport functions, delivers and receive data to/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 data.

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 devices and gateway, which access the MOC capabilities hosted in MOC gateway via ACI;
- MOC applications hosted in MOC devices, which access the MOC capabilities hosted in those same MOC devices via ACI;
- MOC applications hosted in the MOC service domain, which access the NGN via ANI.
- MOC applications hosted in the MOC service domain, which access MOC capabilities of other networks via NNI.

MOC applications hosted in MOC devices and gateways can be invoked by MOC end user and other MOC applications, e.g. MOC applications hosted in the MOC service domain.

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

The service interface across ACI is used to provide interaction in the MOC device domain between MOC capabilities of devices and gateway and MOC applications of devices and gateway. The service interface across ACI 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 enable the following functions:

- Registration of MOC devices and gateway 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 gateway) between MOC capabilities and applications);
- MOC devices and gateway's requests of group creation, deletion and members' listing.

11.4.2 Service interface requirements across UNI

The service interface across UNI 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 resources provided by the MOC device domain to the MOC capabilities in NGN domain.

UNI is required to enable the following functions:

- Registration of MOC capabilities in the MOC device domain to the MOC capabilities in the NGN domain;
- Request from MOC devices of the execution of a specific task to be performed by a MOC application;
- Subscription and notification of specific events from/to the MOC device domain;
- Requests of group creation, deletion and members' listing.

11.4.3 Service interface requirements across ANI

The service requests initiated by MOC applications are sent to the MOC capabilities in NGN domain via ANI. The service interface across ANI is required to provide the interaction between MOC applications in the MOC service domain and MOC capabilities in the NGN domain.

ANI is recommended to support standardized APIs for exposing resources provided by the NGN domain to MOC applications.

ANI is required to enable the following functions:

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

11.4.4 Service interface requirements across NNI

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

- 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 relevant as it implies only transport level interaction.

12 Security considerations

Security requirements for MOC applications are described in clause 8.14.

Security requirements for the NGN domain are provided in clause 9.2.5.

Security requirements for the MOC device domain are provided in clause 10.7.

Appendix I

Actors and related roles in the MOC ecosystem

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

The following identifies different actors of the MOC ecosystem and the business roles (cf. clause 6.3) that they can play:

- The “carrier” actor. The "carrier" actor plays the role of network provider. Depending on the business scenario, the "carrier" actor may also play the role of MOC application provider, MOC platform provider and MOC device 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 may also play (but is not limited to) the role of MOC platform provider;
- The "3rd party device provider" actor. The "3rd party device provider" actor plays the role of MOC device provider. Examples of 3rd party device providers include device operators, end users. The "3rd party device provider" actor may also play (but is not limited to) the roles of MOC platform provider, MOC application provider and MOC application customer.

Appendix II

MOC use cases

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

II.1 E-Health

E-Health is a relatively recent term used to designate healthcare practices supported by electronic processes and communications.

Figure II-1 shows an example of E-Health service configuration.

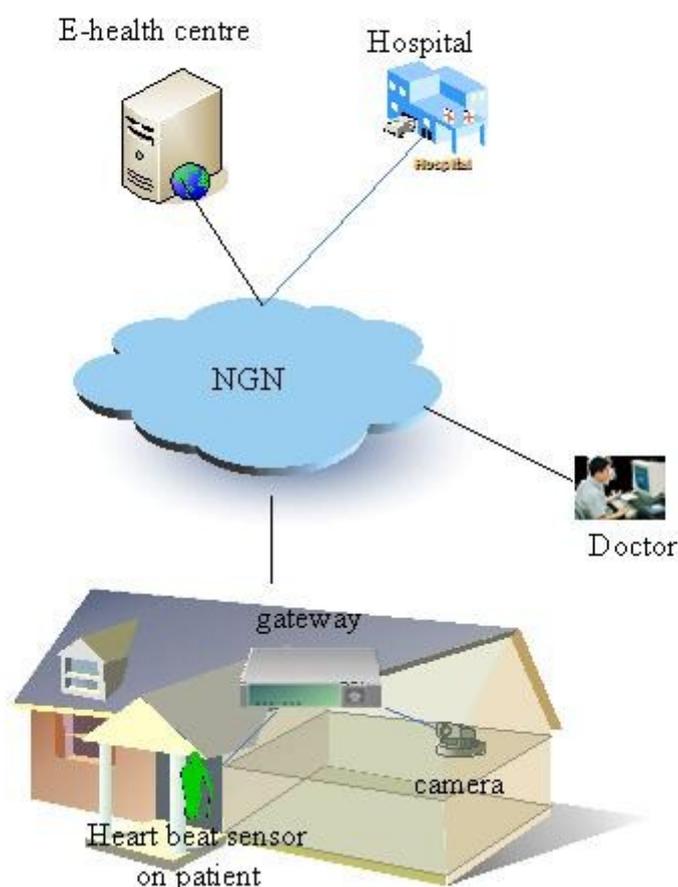


Figure II-1 - E-Health service configuration

Various types of devices are involved in the provisioning of E-Health services. Some of these devices only collect data and interact with the network (e.g. heart beat sensors), others can interact with in a bi-direction (e.g. cameras), some devices usually generate small amount of data (e.g. thermometers), while others may deal with multimedia streaming (e.g. cameras) or, deal with call session control (e.g. SIP terminals supporting video calls). Some devices may even work as both gateway and sensor-like service platforms.

The E-Health devices gather data and send them to the relevant parties, such as the E-Health centre in Figure II-1. Hospitals, doctors and families can subscribe to the service to get raw or process data.

The devices associated with patients can access to network directly or via gateway(s) (e.g., home gateway or gateway worn on body):

- 1) When the patients stay in an indoor environment, the devices can access the network via a single static home gateway or via multiple dynamic home gateways (in this second case the patients can move and access the network via different gateways);
- 2) When the patients roam outdoor, the devices can access to the network directly via a mobile network or indirectly via the gateway worn on body.

The following technical challenges need to be considered for E-Health:

- Grouping should be supported. This is useful, for instance, for multiple patients with the same type of disease, or in case of a single patient, to manage a set of devices which can be managed in group mode;
- Optimized traffic control should be supported. For example, detected data may be very small and need to be reported to network every hour: in such case, it is a waste of resources to be permanently connected to the network. The network should be optimized in terms of traffic control, and, in such case, traffic could be delivered, for example via user plane signalling without data-dedicated IP bearer. Additionally, devices on a patient might stay in sleepy mode and wake up when the doctor needs to diagnose the patient from remote;
- Different mobility levels should be supported. For instance, in case of patients with low mobility (moving not frequently in large areas), it is a waste of resources to activate full mobility management capabilities;
- Device activation and management from remote should be supported. For example, devices in sleepy mode would be waked up only when the doctor needs to diagnose the patient from remote;
- Time control should be supported. For instance, devices on patients may collect a lot of data but don't always need to report them each at every collection as data may be not very critical, e.g. only for routine examination. In these scenarios, the network can allocate specific time slots for the devices' data reporting (the devices cannot report data during other time periods or are charged at higher rates in those periods);
- Device profiles should be supported. Patient may buy new devices and connect them to the network dynamically: device related information should be included in the device profile and be updated dynamically to enable the network authentication and control of the newly-added devices and their removal;
- Devices behind a gateway should be able to be identified by the network. The gateway might provide only a bearer channel and act as a data aggregator for the devices connected to it or might provide service control for the devices connected to it. In the first case, the devices connected to the gateway should be controlled by the network, or by both network and gateway;
- Proprietary devices should be supported. There are plenty of proprietary devices and gateways running in networks: adaptation to existing proprietary devices and gateways should be supported;
- Service profile should be supported. Patients are usually not very familiar with the services offered by the different hospitals, they can usually just logon to E-Health centre's portal and access services, whereas the E-Health centre is usually familiar and can determine the target hospitals based on their professional knowledge. There might be one or multiple hospitals providing medical

services to a patient jointly. In other words, when the devices on a patient report data to the E-Health centre, the centre can intelligently help the patient to select the best target hospitals, and route the data to those hospitals for joint diagnosis. Multimedia call control session might be needed in this scenario, including audio, video, text chatting, etc. The devices should actually interact also with multiple applications.

When doctors diagnose and provide health care services remotely, they usually need also the existing internal disease diagnostics system or database system of the hospital for assistance: data reported from devices maybe input to the existing hospital internal system. In this case, the devices should be interoperable with existing systems (e.g., data format, service capabilities invocation, etc.), that is the E-Health system should be able to collaborate and inter-work with the existing application systems which are usually heterogeneous;

- Traffic load balancing should be taken into consideration in order to cope with particular situations. For instance, because of the varying distribution of the patients, there are relatively high rates of patients in geriatric wards, old communities and some specific cities than in typical cities. The network should be able to handle accordingly the system imbalance in case of specific situation of high traffic or service load, especially for video-like services (for example, when a lot of patients use remote video diagnosis).

II.2 Tsunami warning service

Tsunami warning system is used to detect tsunamis and issue warnings to prevent loss of life and property.

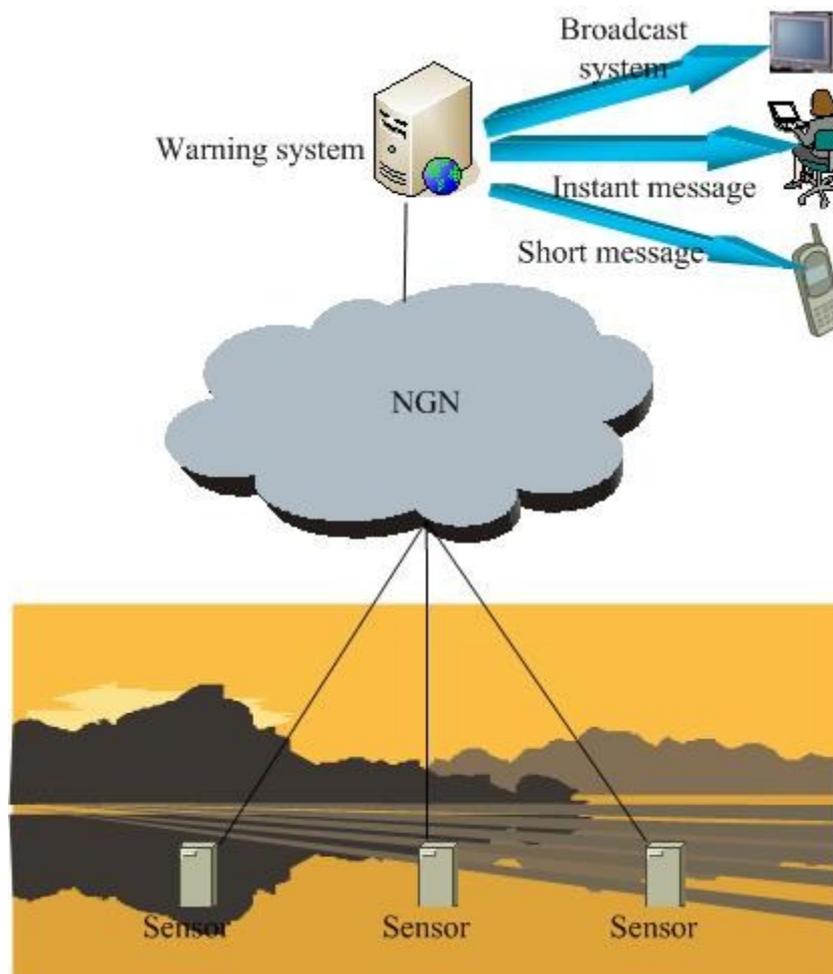


Figure II-2 - Tsunami warning service configuration

As shown in Figure II-2, it consists of two equally important components: a network of sensors to detect tsunamis and a communications infrastructure to issue timely alarms to help evacuation of coastal areas. Detection and prediction of tsunamis is only half the work of the system. The other equal importance is the ability to warn the populations of the areas that will be affected. To save lives more certainly, proper guidance for escape according to their situation in danger (e.g., time, place, and occasion) should be considered. For a visitor who comes to an unfamiliar area at night, a simple alarm is not enough to escape to the safe place. 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 networks (e.g. radio network, television network) and dedicated communication systems (e.g. sirens);
- Delivery of emergency information, including both the primary information generated by the detector and the secondary information transferred to the target population;
- Delivery of emergency information over multiple networks, including reliable and unreliable bearers (e.g., communication through satellite system) to maximize the probability of the delivery;

NOTE - Information integrity which might be compromised by reliable and unreliable bearers needs further study

- System robustness. i.e., the system should support information bursting within a short while due to a large number of machines (e.g., emergency detectors or sensors) within an area;
- Prioritized delivery of emergency information, i.e., emergency message for earthquake, should be prioritized comparing with other service messages.

II.3 Motorcade Management

Figure II-3 shows a typical service configuration for motorcade management.

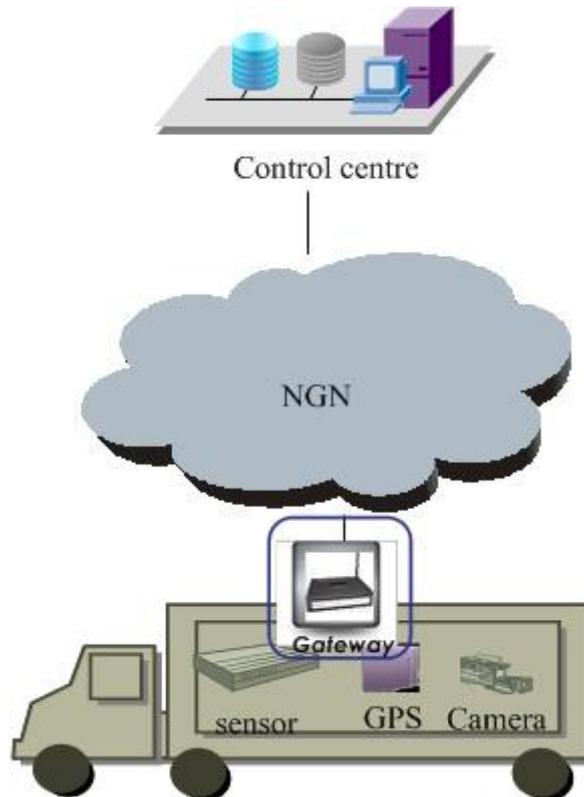


Figure II-3 - Typical Motorcade Management service configuration

Every bus is equipped with devices and gateway which have the same characteristics. The control centre gathers data related to location, speed and situation from the sensors, global positioning system (GPS) terminal and cameras of the bus. Data aggregated through a gateway located in the bus are transmitted to the NGN using wireless access.

The dynamic time table can be pushed to the monitor screen on the bus stop by the control centre according to the location information collected from the bus.

When a sensor on the bus detects an abnormal situation, such as smell of gasoline, an alarm indication is sent to the control centre.

Bus always has a fixed route which means it should not move out the pre-defined roads. When a bus moves out of a particular area, an application should be triggered. For example, a call may be made to the bus driver, or an alert indication may be pushed to the bus administrator while the bus moves out of the area.

In this use case, the service is required to support:

- Location based service: an application should be triggered when devices are in or out of a particular area;
- Prioritized service level. For example, alarm indication should be prioritized comparing with other data;
- Group management for devices with the same characteristics.

II.4 Smart home

Smart home usually involves a mix of different devices and applications, such as real-time or near real-time sensors, power outage notification, and power quality monitoring.

Figure II -4 shows a typical “smart home” configuration.

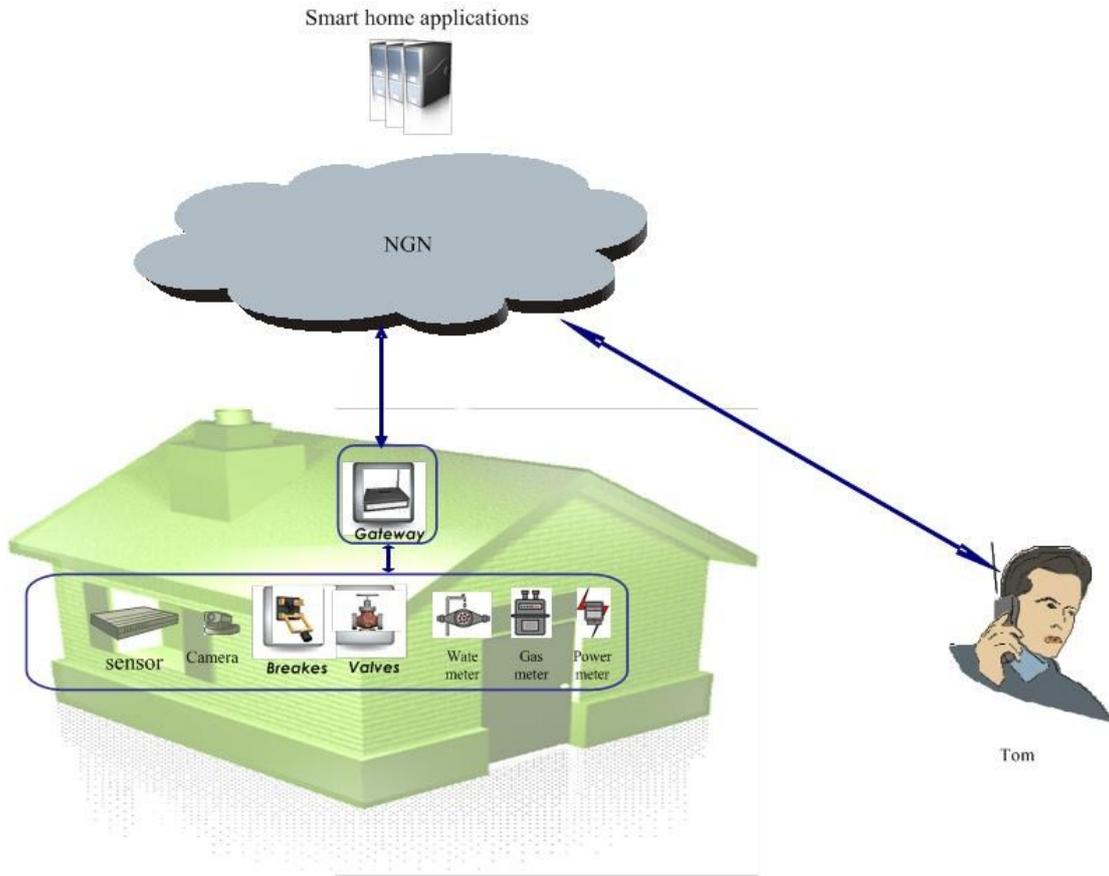


Figure II -4 - Typical smart home service configuration

As shown in Figure II-4, a “smart home” scenario often refers to devices (e.g. smoke sensor, electricity meters, gas meters, etc.) which are connected to a smart home application platform via a gateway located in the smart home. The data centre collects data from the “smart home” devices and is able to control these devices remotely via the gateway. In this scenario, Tom’s house information related to power, gas and water consumption can be collected and reported to the smart home applications platform. At the same time, Tom can manage application related policy of his home using the smart home applications and the application related policy can be sent to MOC devices in order to execute according to Tom’s requirements.

For example, Tom defines the application related 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 an evidence of crime).

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 smoke sensor) sends an alarm message to Tom directly. Upon reception of this information, Tom initiates a video communication

with the camera to check the status of the kitchen, and to tell his son how to use the fire extinguisher or to exit. For privacy and security reasons, the camera is only connected and controlled by members of Tom's family.

In this use case, the service is required to support:

- Enhanced video/audio based capabilities, such as concurrent video streaming and local-breakout;
- Group management for MOC devices with same characteristics, for example, power meter in different smart homes;
- Message broadcasting and multicasting based on specific characteristics, such as group and location, to support functions such as firmware upgrading.

II.5 Integration with Internet services

There are many attractive services emerging in the Internet, such as social network services (SNS). MOC applications should be able to work with those Internet services to ensure that customers can use the MOC applications with existing popular Internet services. Integrated with Internet services, MOC applications themselves will extend their value chains and attract more customers.

In some integration scenarios, MOC capabilities should be able to apply data detection rules (i.e., setting rules) to the MOC devices and gateway. Once detected, the data should be transferred to the MOC capability in a defined format. The formatted data facilitate the MOC capability to communicate smoothly with the Internet services that provide publishing services.

Figure II-5 shows an example use case of the integration of MOC application and Internet service.

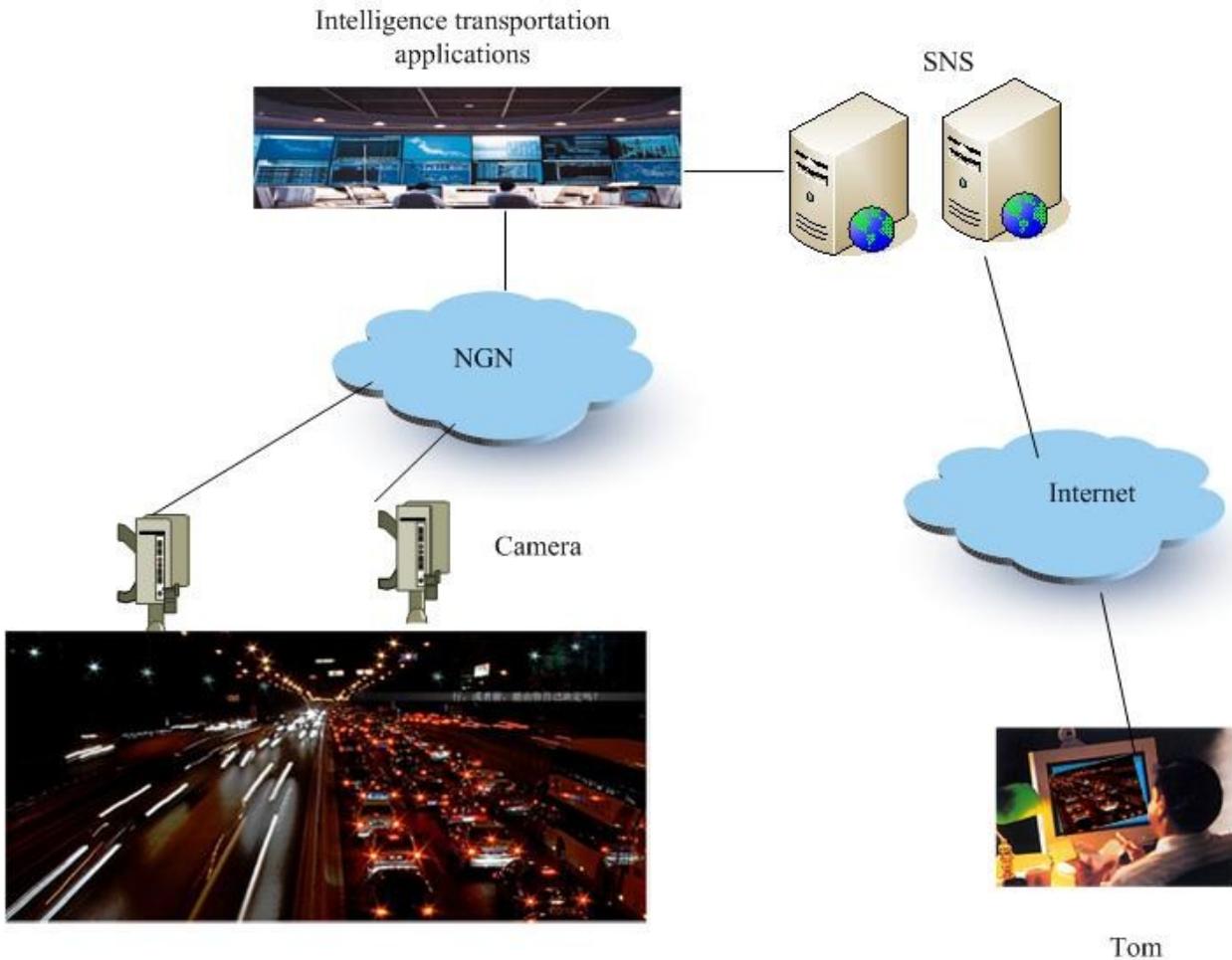


Figure II-5 - Typical internet service configuration

A MOC application provider offers intelligence transportation service for customers. The service allows the customers to access their interested content via SNS with their preferred rules (e.g. publishing times). The provider collects the content by MOC application and provides it for the customers via SNS according to the customers' rules.

Tom finds that the intelligence transportation service provides real time pictures and videos of city traffic captured by the cameras on the streets and that information is provided via SNS. Tom subscribes to this service (e.g. regularly updated every five) and receives the instantaneous traffic information on his SNS.

The service updates the information via SNS according to Tom's preference. Tom can know the highway traffic information on his way to home.

In this use case, the service is required to support:

- Integration with Internet services using the MOC capabilities;
- Setting rules to detect the MOC devices and gateway's data and transfer the data with defined format to the capability which is used to communicate with the Internet services for publishing;
- Enabling customers to access relevant MOC content via the Internet services with defined rules;
- Detecting the relevant MOC content and provide it to the Internet services based on the rules;
- Communicating with the Internet services to exchange the information.

Bibliography

The following documents contain information that may be valuable to the reader of this Recommendation. They provide additional information about topics covered within this Recommendation, but are not essential for an understanding of this Recommendation.

- [b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.
- [b-ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.
- [b-ITU-T Y.2213] Recommendation ITU-T Y.2213 (2008), *NGN service requirements and capabilities for network aspects of applications and services using tag-based identification*
- [b-ITU-T YSup.7] ITU-T Y-series Recommendations – Supplement 7 (2008), *Supplement on NGN release 2 scope*
- [b-ITU-T Q.1741.7] Recommendation ITU-T Q.1741.7 (2011), *IMT-2000 references to Release 9 of GSM-evolved UMTS core network*
- [b-ETSI TS 102 689] ETSI TS 102 689 V1.1.2 (2011-05) *Machine-to-Machine communications (M2M); M2M service requirements*
- [b-ETSI TS 102 690] ETSI TS 102 690 V0.12.3 (2011-06) *Machine-to-Machine communications (M2M); Functional architecture*
- [b-3GPP TS 22.368] 3GPP TS 22.368 V 11.3.0 (2011-09) *Service requirements for Machine-Type Communications (MTC);*
- [b-3GPP2-S.R0141-0] 3GPP2 S.R0141-0 V.1.0 (2010-12) *Machine-to-Machine (M2M) Communication for cdma2000 Networks*