International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2026

(07/2012)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional architecture models

# Functional requirements and architecture of the next generation network for support of ubiquitous sensor network applications and services

Recommendation ITU-T Y.2026

ITU-T Y-SERIES RECOMMENDATIONS

**GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS**

| | |
|---|---|
| GLOBAL INFORMATION INFRASTRUCTURE | |
| General | Y.100–Y.199 |
| Services, applications and middleware | Y.200–Y.299 |
| Network aspects | Y.300–Y.399 |
| Interfaces and protocols | Y.400–Y.499 |
| Numbering, addressing and naming | Y.500–Y.599 |
| Operation, administration and maintenance | Y.600–Y.699 |
| Security | Y.700–Y.799 |
| Performances | Y.800–Y.899 |
| INTERNET PROTOCOL ASPECTS | |
| General | Y.1000–Y.1099 |
| Services and applications | Y.1100–Y.1199 |
| Architecture, access, network capabilities and resource management | Y.1200–Y.1299 |
| Transport | Y.1300–Y.1399 |
| Interworking | Y.1400–Y.1499 |
| Quality of service and network performance | Y.1500–Y.1599 |
| Signalling | Y.1600–Y.1699 |
| Operation, administration and maintenance | Y.1700–Y.1799 |
| Charging | Y.1800–Y.1899 |
| IPTV over NGN | Y.1900–Y.1999 |
| NEXT GENERATION NETWORKS | |
| **Frameworks and functional architecture models** | **Y.2000–Y.2099** |
| Quality of Service and performance | Y.2100–Y.2199 |
| Service aspects: Service capabilities and service architecture | Y.2200–Y.2249 |
| Service aspects: Interoperability of services and networks in NGN | Y.2250–Y.2299 |
| Numbering, naming and addressing | Y.2300–Y.2399 |
| Network management | Y.2400–Y.2499 |
| Network control architectures and protocols | Y.2500–Y.2599 |
| Packet-based Networks | Y.2600–Y.2699 |
| Security | Y.2700–Y.2799 |
| Generalized mobility | Y.2800–Y.2899 |
| Carrier grade open environment | Y.2900–Y.2999 |
| FUTURE NETWORKS | Y.3000–Y.3499 |
| CLOUD COMPUTING | Y.3500–Y.3999 |

*For further details, please refer to the list of ITU-T Recommendations.*

# Recommendation ITU-T Y.2026

## Functional requirements and architecture of the next generation network for support of ubiquitous sensor network applications and services


**Summary**

Recommendation ITU-T Y.2026 includes functional requirements and architecture of the next generation network (NGN) for the support of ubiquitous sensor network (USN) applications and services. This Recommendation is based on the capabilities defined in Recommendation ITU-T Y.2221.



**History**

| Edition | Recommendation | Approval | Study Group |
|---|---|---|---|
| 1.0 | ITU-T Y.2026 | 2012-07-29 | 13 |

**Keywords**

Frameworks, functional architecture, sensor(s), sensor network(s), USN.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

## Table of Contents

# Recommendation ITU-T Y.2026

## Functional requirements and architecture of the next generation network for support of ubiquitous sensor network applications and services

### 1 Scope

This Recommendation, which is based on [ITU-T Y.2012], covers extended features of the next generation network (NGN) for the support of ubiquitous sensor network (USN) applications and services. This Recommendation describes functional requirements, a functional architecture and functional entities in order to support the NGN service requirements and capabilities defined in [ITU-T Y.2221].

This Recommendation covers:

- Functional requirements and functions to support the NGN capabilities defined in [ITU-T Y.2221]
- A functional architecture and entities of the NGN to support USN applications and services

### 2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

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

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 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.

**3.1.2 sensor network** [ITU-T Y.2221]: A network comprised of interconnected sensor nodes exchanging sensed data by wired or wireless communication.

**3.1.3 sensor node** [ITU-T Y.2221]: A device consisting of sensor(s) and optional actuator(s) with capabilities of sensed data processing and networking.

**3.1.4 ubiquitous sensor network (USN)** [ITU-T Y.2221]: A conceptual network built over existing physical networks which makes use of sensed data and provides knowledge services to anyone, anywhere and at anytime, and where the information is generated by using context awareness.

**3.1.5 USN end-user** [ITU-T Y.2221]: An entity that uses the sensed data provided by USN applications and services. This end-user may be a system or a human.

**3.1.6 USN gateway** [ITU-T Y.2221]: A node which interconnects sensor networks with other networks.

## 3.2 Terms defined in this Recommendation

None.

# 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABG-FE Access Border Gateway Functional Entity

AN-FE Access Node Functional Entity

ASF&SSF Application Support Functions and Service Support Functions

AS-FE Application Support Functional Entity

CAF Charging and Accounting Functions

EN-FE Edge Node Functional Entity

IP Internet Protocol

MLM-FE Mobile Location Management Functional Entity

MMCF Mobility Management and Control Functions

NACF Network Attachment Control Functions

NAC-FE Network Access Configuration Functional Entity

NGN Next Generation Network

OSE Open Service Environment

QoS Quality of Service

RACF Resource and Admission Control Functions

SAA-FE Service Authentication and Authorization Functional Entity

SC&CDF Service Control and Content Delivery Functions

SCF Service Control Functions

SCP-FE Service and Content Protection Functional Entity

SUP-FE Service User Profile Functional Entity

TAA-FE Transport Authentication and Authorization Functional Entity

TLM-FE Transport Location Management Functional Entity

TRC-FE Transport Resource Control Functional Entity

TUP-FE Transport User Profile Functional Entity

USN Ubiquitous Sensor Network

## 5 Conventions

None.

## 6 Functional requirements and functions of the NGN for USN applications and services

### 6.1 NGN functional requirements

[ITU-T Y.2221] describes the NGN service requirements and capabilities to support USN applications and services, and clause 8.1 of [ITU-T Y.2221] specifically states the following requirements for extensions or additions to NGN capabilities to support USN applications and services:

- Network management
- Profile management
  - Service profile

    NOTE 1 – Service profile requirement can be supported by existing NGN capabilities. See clause I.1.
  - Device profile
- Open service environment (OSE)
  - Service registration and discovery
  - Inter-working with service creation environments

    NOTE 2 – This Recommendation does not take these requirements into consideration. See clause I.1.
- Quality of service (QoS)
  - Application traffic control

    NOTE 3 – Application traffic control can be supported by existing NGN capabilities. See clause I.1.
- Privacy

  NOTE 4 – This Recommendation does not take this requirement into consideration. See clause I.1.

In addition to these capabilities, clause 8.2 of [ITU-T Y.2221] explains that the following capabilities are supported by the existing NGN capabilities to support USN applications and services:

- Open service environment
  - Service composition and coordination

    NOTE 5 – This Recommendation does not take this requirement into consideration. See clause I.1.
- Quality of service
  - Differentiated QoS and data prioritization
- Connectivity
- Location management
- Mobility
- Security
- Identification, authentication and authorization
- Accounting and charging

Appendix I describes requirements for the support of USN applications and services in NGN and allocates the corresponding functions of NGN to satisfy the requirements.

## 6.2 Functional architecture model

Figure 1 depicts the overall diagram of USN architecture, which uses NGN as a backbone network.

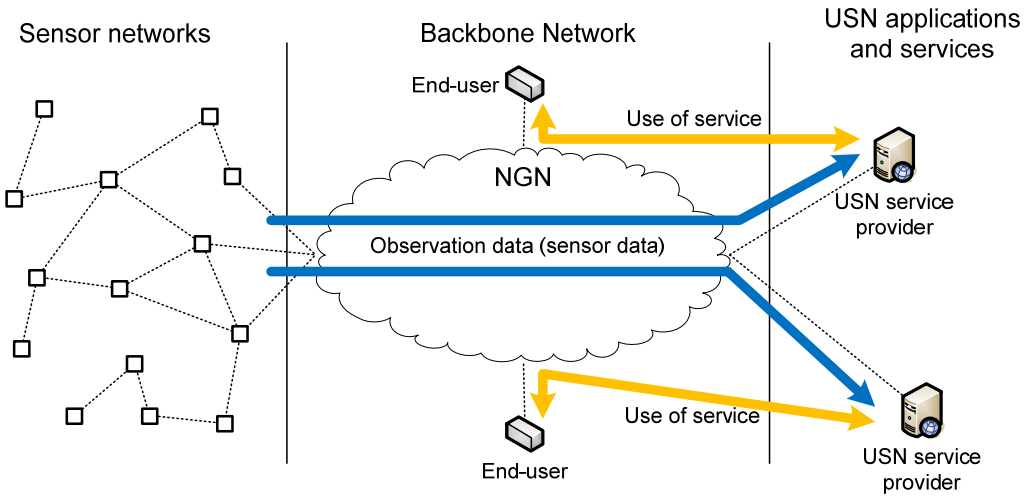


**Figure 1 – Overall USN architecture**

The sensor networks gather information about their physical surroundings and deliver this information to USN service providers through NGN. The USN service providers create USN services using this information and provide them to USN end-users via NGN. The USN end-users utilize USN services through NGN.

As a backbone network, NGN provides the capabilities for the support of USN applications and services in the transport stratum functions, the service stratum functions, the management functions and the end-user functions.

Figure 2 shows the overall functional architecture model of the NGN to support USN applications and services. More specifically, the figure shows the functions required for the support of USN applications and services. Appendix I describes requirements for the support of USN applications and services in NGN and allocates the corresponding functions of NGN to satisfy the requirements.

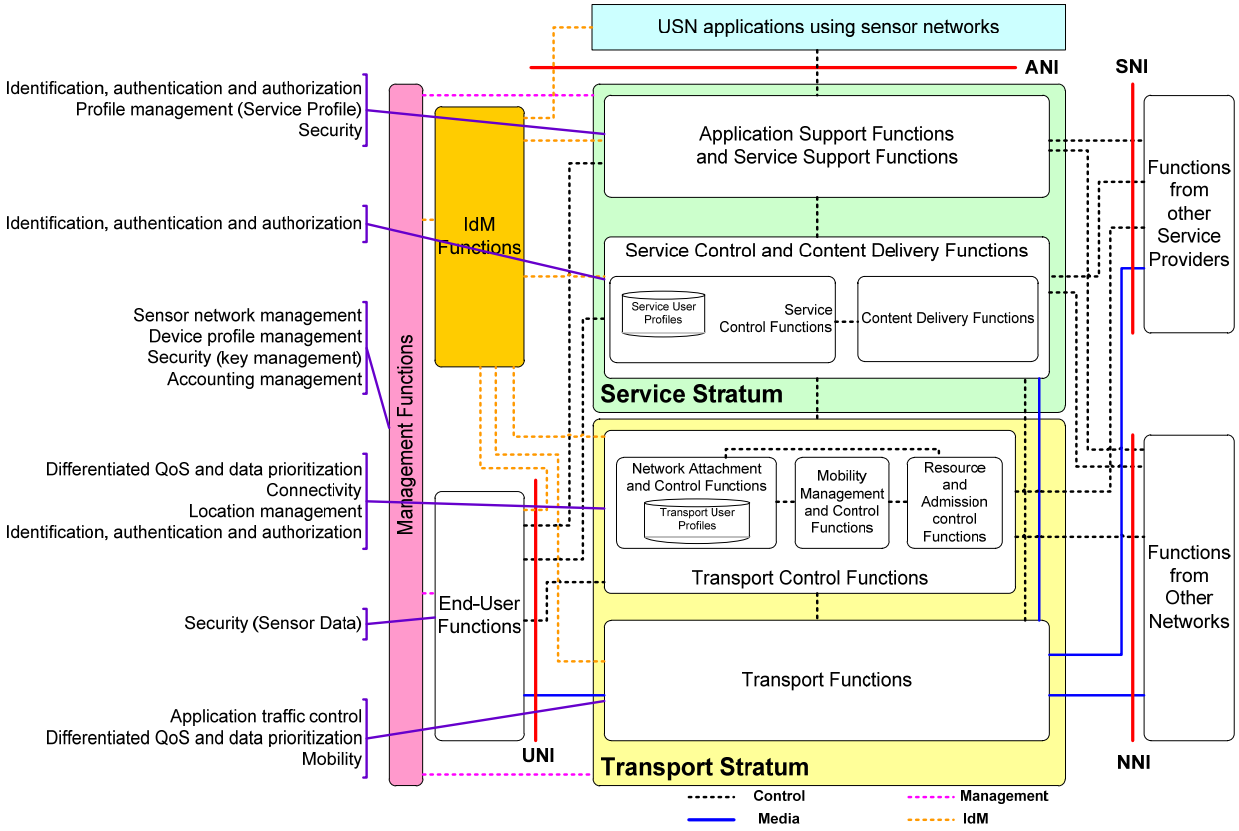


**Figure 2 – Overall functional architecture model**

As seen in Figure 2, there are no additional functions beyond [ITU-T Y.2012] to support requirements for USN applications and services. However, some NGN functions should be extended to support requirements in terms of functionalities. Clause 6.3 describes NGN functions to support USN applications and services.

## 6.3 Functions to support USN applications and services

This clause describes how the functional requirements identified in clause 6.1 are supported in the functional architecture model shown in clause 6.2. This clause focuses on the NGN capabilities which need the extensions of NGN functions to support USN applications and services.

The extension of NGN functions means that the NGN functions defined in [ITU-T Y.2012] should support additional capabilities for the requirements of USN applications and services. The extension of NGN functions can be achieved by implementation of additional capabilities of each stratum function.

### 6.3.1 Transport stratum functions

The transport stratum functions are required to be extended to support requirements of USN applications and services. The extensions of the transport stratum functions are given in the following clauses.

#### 6.3.1.1 Transport functions

The following functional requirements are supported by the existing capabilities of the transport functions [ITU-T Y.2012]:

- Application traffic control requirement:

  The access network functions, edge functions and core transport functions are used for satisfying an application traffic control requirement which requests the management of transaction volume generated by the USN end-users.

- Differentiated QoS and data prioritization requirement:

  USN mission-critical applications and services should be carefully managed. For example, emergency notification of a fire case must be delivered by a time-critical and reliable way to appropriate national disaster monitoring systems. The access network functions, edge functions and core transport functions provide differentiated QoS and data prioritization capabilities.

#### 6.3.1.2 Transport control functions

There are no extended capabilities in the transport control functions to support USN applications and services. The following functional requirements are supported by the transport control functions [ITU-T Y.2012]:

- Differentiated QoS and data prioritization requirement:

  As described in clause 6.3.1.1, USN applications and services require differentiated QoS and data prioritization. The resource and admission control functions (RACF) provides this capabilities in cooperation with the transport functions.

- Connectivity requirement:

  Both IP-based and non IP-based sensor networks can connect to NGN. When a non IP-based sensor network connects to NGN, an IP-capable gateway is used. The network attachment control function (NACF) provides connectivity to IP-based and non-IP based sensor networks through gateways.

- Location management requirement:

  The NACF provides a location management capability at the IP layer. If a sensor network uses IP addresses directly or a USN gateway provides IP-based connectivity, the location information management of sensor networks at the IP layer is supported by the NACF.

- Mobility requirement:

  The access network functions provide a mobility capability of a sensor network as well as mobility of a sensor node within a sensor network or across sensor networks. If a sensor network is based on IP technologies, the mobility management and control functions (MMCF) provide functions for the support of IP-based mobility of a sensor network as well as a sensor node.

- Identification, authentication and authorization:

  The NACF provides authentication of the USN end-users and authorization of network access.

### 6.3.2 Service stratum functions

The service stratum functions are required to be extended to support requirements of USN applications and services. The extensions of the service stratum functions are given in the following clauses.

#### 6.3.2.1 Service control and content delivery functions

The following functional requirements are supported by existing service control and content delivery functions [ITU-T Y.2012]:

- Identification, authentication and authorization requirement:

  The service control functions (SCF) support authentication and authorization functions for the USN end-users at the service level.

#### 6.3.2.2 Application support functions and service support functions

There are no extended capabilities in the application support functions and service support functions to support USN applications and services.

The following functional requirements are supported by existing application support functions and service support functions [ITU-T Y.2012]:

- Identification, authentication and authorization requirement:

  The application support functions and service support functions (ASF&SSF) provide authentication and authorization to access the services at the application level.

- Profile management requirement for registration and discovery of service:

  [ITU-T Y.2221] specifies that the service profile for service registration and discovery requires the extension of NGN capabilities. However, [ITU-T Y.2012] defines that the ASF&SSF, especially the application support functional entity (AS-FE), provides generic application server functions such as service selection and service discovery.

- Security:

  Application support functions and service support functions provide the protection of content (sensor data).

### 6.3.3 Management functions

The management functions are required to be extended to support requirements of USN applications and services. The extensions of the management functions are as follows:

- Sensor network management requirement:

  IP-based and non-IP-based sensor networks using various types of wired and/or wireless connection can coexist in USN applications and services. Non-IP-based sensor networks are often managed through their gateway. IP-based sensor networks include the case of a single sensor node directly connected to NGN, although sensor networks are often managed as a set. The management functions are required to manage IP-based sensor networks as well as non IP-sensor networks.

- Profile management (device profile) requirement:

  In USN applications and services, a device profile consisting of the information of sensor networks and/or sensor nodes should be provided and managed. As there are various types of sensors, sensor nodes and sensor networks, device profiles would help to manage a large number of heterogeneous nodes and networks. The information of device profiles may include sensor network identifier, device identifier, device types, capabilities and location. The management functions may support device profile management.

However, the following functional requirements are supported by existing management functions [ITU-T Y.2012]:

- Security requirement:

  Security management of USN applications and services including key management is supported by the management functions.

- Accounting and charging requirement:

  Different accounting and charging requirements might have to be addressed depending on the scenarios of USN applications and services. The management functions are required to support different accounting and charging policies according to different data transaction types of USN applications and services.

#### 6.3.4 End-user functions

Existing end-user functions are required to support the following functions:

- Security requirement:

  Sensor data security within a sensor network is provided by the end-user functions.

## 7 Functional architecture of the NGN for USN applications and services

The extensions and additions of the functional entities defined in [ITU-T Y.2012] are required for the support of USN applications and services. Based on the functions described in clause 6.3, this clause identifies the extensions and additions of the functional entities of the NGN functional architecture illustrated in Figures 9-2, 9-3 and 9-4 of [ITU-T Y.2012].

### 7.1 Transport processing functional entities

#### 7.1.1 T-2: Access node functional entity (AN-FE)

- Application traffic control requirement:

  The AN-FE supports an application traffic control requirement which requests the management of transaction volume generated by the USN end-users.

- Differentiated QoS and data prioritization requirement:

  The AN-FE supports different QoS and also supports data prioritization capabilities.

#### 7.1.2 T-3: Edge node functional entity (EN-FE)

- Application traffic control requirement:

  The EN-FE supports an application traffic control requirement which requests the management of transaction volume generated by the USN end-users.

- Differentiated QoS and data prioritization requirement:

  The EN-FE supports different QoS and also supports data prioritization capabilities.

#### 7.1.3 T-5: Access border gateway functional entity (ABG-FE)

- Differentiated QoS and data prioritization requirement:

  The ABG-FE supports different QoS and also supports data prioritization capabilities.

### 7.2 Transport control functional entities

#### 7.2.1 T-10: Network access configuration functional entity (NAC-FE)

- Connectivity requirement:

  The NAC-FE provides connectivity to IP-based and non-IP based sensor networks through gateways.

#### 7.2.2 T-11: Transport authentication and authorization functional entity (TAA-FE)

- Identification, authentication and authorization:

  The TAA-FE provides authentication of the USN end-users and authorization of network access.

#### 7.2.3 T-12: Transport user profile functional entity (TUP-FE)

- Identification, authentication and authorization:

  The TAA-FE provides authentication of the USN end-users and authorization of network access.

#### 7.2.4 T-13: Transport location management functional entity (TLM-FE)

- Location management requirement:

  The TLM-FE provides location management capability at the IP layer. If a sensor network uses IP addresses directly or a USN gateway provides IP-based connectivity, the location information management of sensor networks at the IP layer is supported by the TLM-FE.

#### 7.2.5 T-17: Transport resource control functional entity (TRC-FE)

- Differentiated QoS and data prioritization requirement:

  The TRC-FE provides different QoS and also supports data prioritization capabilities.

#### 7.2.6 T-18: Mobile location management functional entity (MLM-FE)

- Mobility requirement:

  The MLM-FE provides functions for the support of IP-based mobility of a sensor network as well as a sensor node.

### 7.3 Service control functional entities

#### 7.3.1 S-5: Service user profile functional entity (SUP-FE)

- Identification, authentication and authorization:

  The SUP-FE is responsible for storing user profiles, subscriber-related location data and presence status data in the service stratum. A user profile is required to be provided in support of authentication, authorization and so on.

#### 7.3.2 S-6: Service authentication and authorization functional entity (SAA-FE)

- Identification, authentication and authorization:

  The SAA-FE provides authentication and authorization in the service stratum.

### 7.4 Application support functions and service support functions

#### 7.4.1 A-1: Application support functional entity (AS-FE)

- Profile management requirement for service registration and discovery:

  The AS-FE supports generic application server functions including hosting and executing services such as service selection servers and service discovery servers.

#### 7.4.2 A-8: Service and content protection functional entity (SCP-FE)

- Identification, authentication and authorization:

  The SCP-FE provides authentication and authorization in the service stratum.

- Security:

  The SCP-FE provides the protection of the services and content (sensor data).

## 8 Security considerations

Security considerations regarding the functional requirements and architecture of the NGN are addressed in [ITU-T Y.2701].

# Appendix I

## Analysis of service requirements and network capabilities defined in Recommendation ITU-T Y.2221

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

### I.1 Requirements for extensions to NGN capabilities

[ITU-T Y.2221] defines the following requirements to be supported by extended NGN capabilities.

| Requirements | Explanation |
|---|---|
| Network management | • It is required to manage IP-based sensor networks including the case of a single node directly connected to NGN.<br>• It is required to manage non-IP-based sensor networks.<br>• It is required to support configuration and reconfiguration of sensor networks for assurance of connectivity and lifetime management. |
| Profile management for service registration and discovery | • It is recommended to use a standard set of USN service profiles to register and discover USN services.<br>NOTE – [ITU-T Y.2221] specifies that the service profile for service registration and discovery requires the extension of NGN capabilities. However, [ITU-T Y.2012] defines that the ASF&SSF, especially the application support functional entity (AS-FE), provides generic application server functions such as service selection and service discovery.<br>Therefore, a service profile requirement can be supported by existing NGN capabilities. |
| Profile management: Device profile | • It is optional to use device profiles containing sensor network related information. |
| Open service environment: Service registration and discovery | • It is required to support at least one USN service description language and its associated execution framework.<br>• It is recommended to register and discover USN services based on a standard set of USN service profiles.<br>• Registration and discovery of sensor network devices may be supported.<br>• Context-awareness can be optionally supported in service discovery for USN applications and services.<br>NOTE – [ITU-T Y.2221] specifies that service registration and discovery using the service profile under OSE require the extension of NGN capabilities. However, [ITU-T Y.2012] defines that the ASF&SSF, especially the application support functional entity (AS-FE), provides generic application server functions such as service selection and service discovery.<br>Therefore, OSE service registration and discovery requirement can be supported by the existing NGN capability (i.e., ASF&SSF) instead of OSE. |

| Requirements | Explanation |
|---|---|
| Open service environment: Inter-working with service creation environments | • It is recommended to support inter-working with other service creation environments for the creation of USN applications and services<br>NOTE – From the viewpoint of USN applications and services, NGN may be regarded as an intermediate network providing connectivity, data delivery and management. Service creation under OSE provides NGN service creation, not creation of USN applications and services. USN service creation is provided by other service providers and not the NGN.<br>Therefore this Recommendation does not take this requirement into consideration. |
| Quality of service: Application traffic control | • It is required to manage the transaction volume generated by USN applications and services.<br>• It is recommended to be able to avoid access concentration to a single resource.<br>NOTE – [ITU-T Y.2221] specifies that QoS-application traffic control requires the extension of NGN capabilities. However, [ITU-T Y.2012] defines that access network functions and edge functions provide QoS and traffic control.<br>Therefore QoS-application traffic control requirement can be supported by existing NGN capabilities. |
| Privacy | • There should be an option for privacy-enhanced multi-hop routing mechanisms (information on originating node identifier (ID), time and location should not be revealed – at least not totally – to intermediate nodes).<br>• There should be an operating option to de-correlate sensor activity patterns (revealing sensitive context information) from the ensuing communication traffic patterns.<br>NOTE – [ITU-T Y.2221] specifies that privacy protection should be supported by NGN. However, this requirement needs an end-to-end (from sensor node/sensor network to application) security mechanism. The main role of NGN for supporting USN applications and services is delivering sensor data to USN applications or delivering control data to sensor networks. From the USN point of view, NGN is an intermediate network and the components of NGN can also be regarded as intermediate nodes.<br>Therefore privacy protection that requires an end-to-end security mechanism cannot be supported by NGN functions and this Recommendation does not take this requirement into consideration. |

## I.2 Requirements supported by existing NGN capabilities

[ITU-T Y.2221] defines the following requirements to be supported by existing NGN capabilities.

| Requirements | Explanation |
|---|---|
| Open service environment: Service composition and coordination | • It is recommended to support service composition and coordination for creation of USN applications and services.<br>NOTE – From the viewpoint of USN applications and services, NGN may be regarded as an intermediate network providing connectivity, data delivery and management. Service composition and coordination under OSE provides NGN service composition and coordination, not USN applications and services. USN service composition and coordination is provided by other service providers than NGN.<br>Therefore this Recommendation does not take this requirement into consideration. |
| Quality of service: Differentiated QoS and data prioritization | • It is recommended to provide differentiated QoS and data prioritization according to the specific USN service requirements. |
| Connectivity | • It is required to support connectivity between sensor networks and infrastructure networks, regardless of the sensor network type, i.e., IP-based or non-IP-based and using various types of wired and/or wireless media connections. This includes the case in IP-based sensor networks of a single sensor node directly connected to the infrastructure networks. |
| Location management | • Location information of sensor networks is recommended to be registered for USN applications and services. Registration can be static or dynamic.<br>• Location information of an individual sensor node can be optionally registered for USN applications and services when the location information of a single sensor node is useful.<br>• Location information is recommended to be trustworthy, hence location discovery and management is recommended to be secure. |
| Mobility | • It is required to support network mobility when a sensor network moves across infrastructure networks.<br>• Infrastructure networks are required to support intra-sensor network mobility and inter-sensor network mobility when location information of a moving sensor node is required to be traced. |

| Requirements | Explanation |
|---|---|
| Security | • It is required to support key management schemes for USN applications and services.<br>• It is recommended to support scalable key management schemes for USN applications and services operating with large sensor networks.<br>• It is recommended to provide security for the aggregated data when sensed data from two or more applications and services are integrated in infrastructure networks for the creation of new services.<br>• The security approaches for the support of USN applications and services are recommended to be consistent with the general approach for security in NGN.<br>• In addition to data security, the USN communication infrastructure is recommended to provide information transport security for protection against well-known passive and active attacks. Protocols for information transport are required to be resilient to attacks.<br>• Depending on the specific USN application security requirements, a means for intrusion detection is required. |
| Identification, authentication and authorization | • It is required to support identification, authentication and authorization for users to access USN applications and services based on the security level of service data.<br>• It is required to support different levels of authentication for different types of data based on the requirements of USN applications and services.<br>• The USN end-users can optionally identify and authenticate network providers and USN service providers. |
| Accounting and charging | • It is required to support different accounting and charging policies according to different data transaction types of USN applications and services. |

## I.3 Mapping table of the requirements and the extended NGN functions

Clause I.1 defines the NGN capabilities to be extended to satisfy the requirements of [ITU-T Y.2221]. This clause allocates proper functions of NGN which are defined in [ITU-T Y.2012] to support the capabilities.

| Requirements | Corresponding functions |
|---|---|
| Network management | • Management functions |
| Profile management: Device profile | • Management functions |

## I.4 Mapping table of the requirements and the existing NGN functions

Clause I.2 defines the existing NGN capabilities to satisfy the requirements of [ITU-T Y.2221]. This clause allocates proper functions of NGN which are defined in [ITU-T Y.2012] to support the capabilities.

| Requirements | Corresponding functions |
|---|---|
| Profile management for service registration and discovery | • Application support functions and service support functions (ASF&SSF) |
| Quality of service: Application traffic control | • Transport functions<br>– Access network functions<br>– Edge functions<br>• Core transport functions |
| Quality of service: Differentiated QoS and data prioritization | • Transport functions<br>– Access network functions<br>– Edge functions<br>– Core transport functions<br>• Transport control functions<br>– Resource and admission control functions (RACF) |
| Connectivity | • Transport control functions<br>– Network attachment control functions (NACF) |
| Location management | • Transport control functions<br>– Network attachment control functions (NACF) |
| Mobility | • Transport functions<br>– Access network functions<br>– Mobility management and control functions (MMCF) |
| Security | • Management functions (security key management)<br>• End-user functions (data security)<br>• Application support functions and service support functions (ASF&SSF) |
| Identification, authentication and authorization | • Transport control functions<br>– Network attachment control functions (NACF)<br>• Service control and content delivery functions (SC&CDF)<br>– Service control functions (SCF)<br>• Application support functions and service support functions (ASF&SSF) |
| Accounting and charging | • Management functions (accounting management)<br>– Charging and accounting functions (CAF) |

# Appendix II

## USN middleware functions provided by NGN

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

[b-ITU-T F.744] describes USN middleware as follows:

- USN middleware is an intermediate entity which provides functions commonly required by different types of USN applications and services. USN middleware receives requests from USN applications and delivers those requests to appropriate sensor networks. Similarly, USN middleware receives sensed data or processed data from sensor networks and delivers them to appropriate USN applications. USN middleware can provide information processing functions such as query processing, context-aware processing, event processing, sensor network monitoring and so on.

NOTE – Detailed descriptions and requirements related to USN middleware are given in [b-ITU-T F.744].

From the description above, it is understood that USN middleware provides accessibility to sensor networks and data between sensor networks and USN applications and services. Also, USN middleware encompasses information processing functions which may be commonly required by various types of USN applications and services.

As described in Appendix I, NGN may be regarded as an intermediate network providing connectivity, data delivery and management. From these facts, USN middleware functions can be implemented by NGN functions.

Figure II.1 depicts the functional model of USN middleware given in [b-ITU-T F.744]. NGN functions may provide basic functions and advanced functions of USN middleware in each stratum of NGN.

However, this Recommendation does not intend to clarify NGN functional entities for providing USN middleware functions. This is out of scope of this Recommendation.

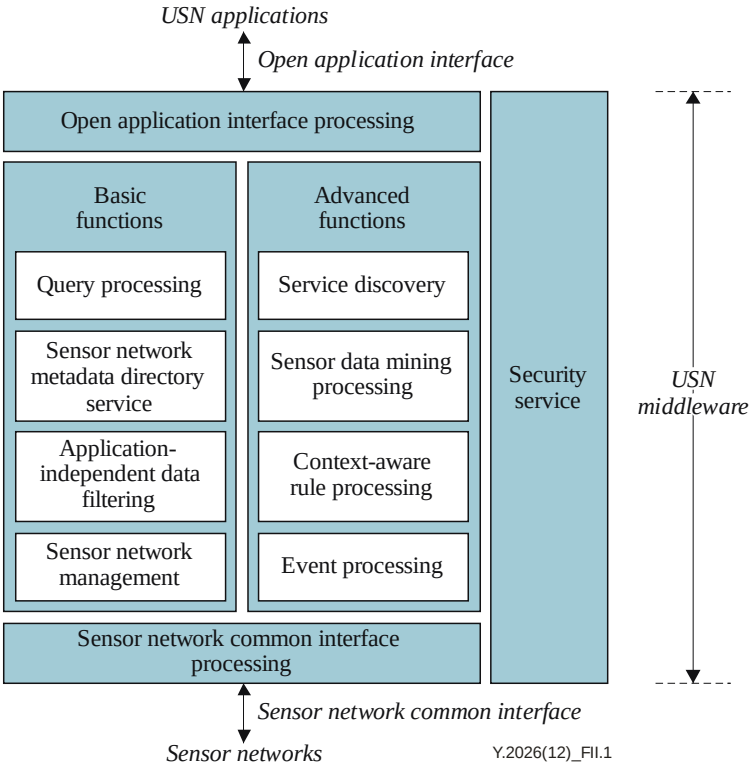


**Figure II.1 – Functional model of USN middleware ([b-ITU-T F.744])**

# Bibliography

[b-ITU-T F.744] Recommendation ITU-T F.744 (2009), *Service description and requirements for ubiquitous sensor network middleware*.

## SERIES OF ITU-T RECOMMENDATIONS

| | |
|---|---|
| Series A | Organization of the work of ITU-T |
| Series D | General tariff principles |
| Series E | Overall network operation, telephone service, service operation and human factors |
| Series F | Non-telephone telecommunication services |
| Series G | Transmission systems and media, digital systems and networks |
| Series H | Audiovisual and multimedia systems |
| Series I | Integrated services digital network |
| Series J | Cable networks and transmission of television, sound programme and other multimedia signals |
| Series K | Protection against interference |
| Series L | Construction, installation and protection of cables and other elements of outside plant |
| Series M | Telecommunication management, including TMN and network maintenance |
| Series N | Maintenance: international sound programme and television transmission circuits |
| Series O | Specifications of measuring equipment |
| Series P | Terminals and subjective and objective assessment methods |
| Series Q | Switching and signalling |
| Series R | Telegraph transmission |
| Series S | Telegraph services terminal equipment |
| Series T | Terminals for telematic services |
| Series U | Telegraph switching |
| Series V | Data communication over the telephone network |
| Series X | Data networks, open system communications and security |
| **Series Y** | **Global information infrastructure, Internet protocol aspects and next-generation networks** |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2013