International Telecommunication Union

ITU-T
TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4213
(11/2021)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Requirements and use cases

Internet of Things requirements and capability framework for monitoring physical city assets

Recommendation ITU-T Y.4213

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

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
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	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.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	**Y.4100–Y.4249**
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.4213

Internet of Things requirements and capability framework for monitoring physical city assets

Summary

Recommendation ITU-T Y.4213 identifies specific IoT requirements for monitoring physical city assets in smart cities. Common requirements of the IoT (Recommendation ITU-T Y.4100), requirements for the interoperability of smart city platforms (Recommendation ITU-T Y.4200) and high-level requirements and reference framework of smart city platforms (Recommendation ITU-T Y.4201) constitute the basis for these specific requirements.

Based on the identified requirements, a capability framework of a city asset monitoring system is provided, composed of city asset monitoring device capabilities, network connectivity management capability, IoT device management capabilities, identifier management capabilities and city asset monitoring service capabilities.

The requirements and capabilities only address technical aspects of the IoT-enabled city infrastructure, but the analysis of specific city assets is beyond the scope of this Recommendation. Other aspects, including regulatory and economic ones, are also out of the scope of this Recommendation.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.4213

Internet of Things requirements and capability framework
for monitoring physical city assets

1 Scope

Monitoring city assets can help smart city administrators to implement planning and control activities (e.g., policies and processes) in order to improve the operational efficiency of city facilities as well as to reduce potential risks to an acceptable level, for the benefits of all smart city stakeholders.

City asset monitoring may benefit from using Internet of things (IoT), especially for asset safeguarding, maintenance and management.

This Recommendation identifies requirements of IoT-enabled city infrastructure and capability framework for monitoring physical city assets, in order to enable an effective asset monitoring in smart cities.

The requirements and capabilities only address technical aspects of the IoT-enabled city infrastructure. Other aspects, including regulatory and economic ones, are out of the scope of this document.

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.4000]   Recommendation ITU-T Y.4000 (2012), *Overview of the Internet of Things*.

[ITU-T Y.4100]   Recommendation ITU-T Y.4100 (2014), *Common requirements of the Internet of things*.

[ITU-T Y.4200]   Recommendation ITU-T Y.4200 (2018), *Requirements for the interoperability of smart city platforms*.

[ITU-T Y.4201]   Recommendation ITU-T Y.4201 (2018), *High-level requirements and reference framework of smart city platforms*.

[ITU-T Y.4212]   Recommendation ITU-T Y.4212 (2021), *Requirements and capabilities of network connectivity management in the Internet of things*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 asset [b-ITU-T F.751.0]: A representation of value. It can be a diamond, a unit of currency, items inside a shipping container, etc. An asset can be physical or virtual.

3.1.2 authentication [b-ITU-T X.811]: The provision of assurance of the claimed identity of an entity.

3.1.3 **authorization** [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.14 **Internet of Things (IoT)** [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.5 **smart city platform (SCP)** [ITU-T Y.4201]: A city platform that offers direct integration of city platforms and systems, or through open interfaces between city platforms and third parties, in order to offer urban operation and services supporting the functioning of city services, as well as efficiency, performance, security and scalability

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API   Application Programming Interface

GNSS   Global Navigation Satellite System

IoT   Internet of things

LBS   Location Based Services

RFID   Radio Frequency Identification

SCP   Smart city platform

WiFi   Wireless Fidelity

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 with which compliance is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "can optionally" and "may" indicate an optional requirement which it is permissible to comply with, 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 Overview of asset monitoring

A city is a large human settlement. Cities generally have high-density facilities for housing, transportation, sanitation, utilities, land use and communication. The high density facilitates interaction between people, government organizations and businesses, benefiting different parties in

the process. These facilities are the physical assets of a city and are addressed by this Recommendation.

NOTE 1 – The typical kinds of physical city assets may include, but are not limited to, environment sanitation facilities, water supply and drainage facilities, energy facilities, transportation facilities, postal and telecommunication facilities and disaster prevention facilities.

Physical city assets continue to evolve with technology and city development. With the support of IoT, city assets' safeguarding, maintenance and management can enable new service experience to be provided to the diversity of users, including but not limited to citizen and city asset operators.

The overview diagram of a physical city asset monitoring system is shown in Figure 1. The physical city asset monitoring system collects data of the physical city assets and provides a set of services to smart city applications and other smart city systems.
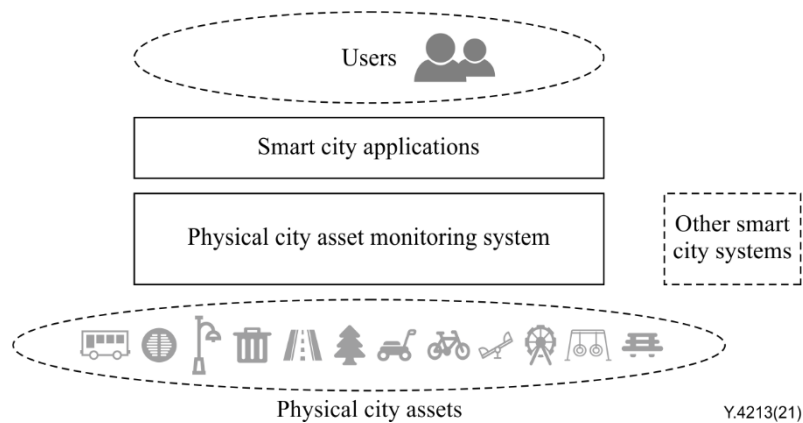

Figure 1 – Overview diagram of a physical city asset monitoring system

7   IoT requirements for monitoring physical city assets

Building on common requirements of the IoT [ITU-T Y.4100], requirements for the interoperability of smart city platforms (SCPs) [ITU-T Y.4200] and high-level requirements and reference framework of SCPs [ITU-T Y.4201], this clause identifies specific IoT requirements for monitoring physical city assets.

7.1   Physical city asset locating

Physical city asset locating is required. Appropriate positioning accuracy is required to be supported in order to meet service requirements.

7.2   Network coverage

To support monitoring physical city assets or to support tracking of their location, it is recommended to provide network coverage in all relevant city spaces.

NOTE – Physical city assets can be situated in many places, for example, city buses can be parked in either outdoor or indoor parking locations or underground parking locations. In order to support city bus location tracking in outdoor, indoor and underground parking locations, appropriate city spaces are required to be covered by the network.

7.3   Network bandwidth

Network bandwidth is required to be appropriately provided in order to satisfy the data transmission requirements.

NOTE – As an example, large network bandwidth is required to be provided in order to support video monitoring for city elevators.

7.4 Network reliability

To support city asset monitoring devices dedicated to emergency support, high reliability is required concerning the associated network infrastructure.

7.5 City asset data sharing

Sharing of city asset related data among smart city systems is recommended as appropriate, e.g., to improve city asset usage efficiency across multiple city stakeholders or in support of specific applications operated by other smart city systems.

7.6 City asset identification

In order to support monitoring city assets and to support recording for each city asset in other smart city systems, it is required to allocate each city asset monitoring device a unique identifier and to provide the ability to associate city asset related information to this identifier. Based on the unique identifier, the city asset related information can be also accessed by other smart city systems.

7.7 City asset related fault diagnosis

To support maintenance of city assets, fault diagnosis for city asset monitoring devices is required to be supported.

7.8 City asset related fault recovery

To support maintenance of city assets, fault recovery from remote for city asset monitoring devices is recommended to be supported.

8 Capability framework for monitoring physical city assets

The capability framework of city asset monitoring system is composed of city asset monitoring device capabilities, IoT device management capabilities, city asset monitoring service capabilities, network connectivity management capabilities and identification capabilities, as shown in Figure 2.
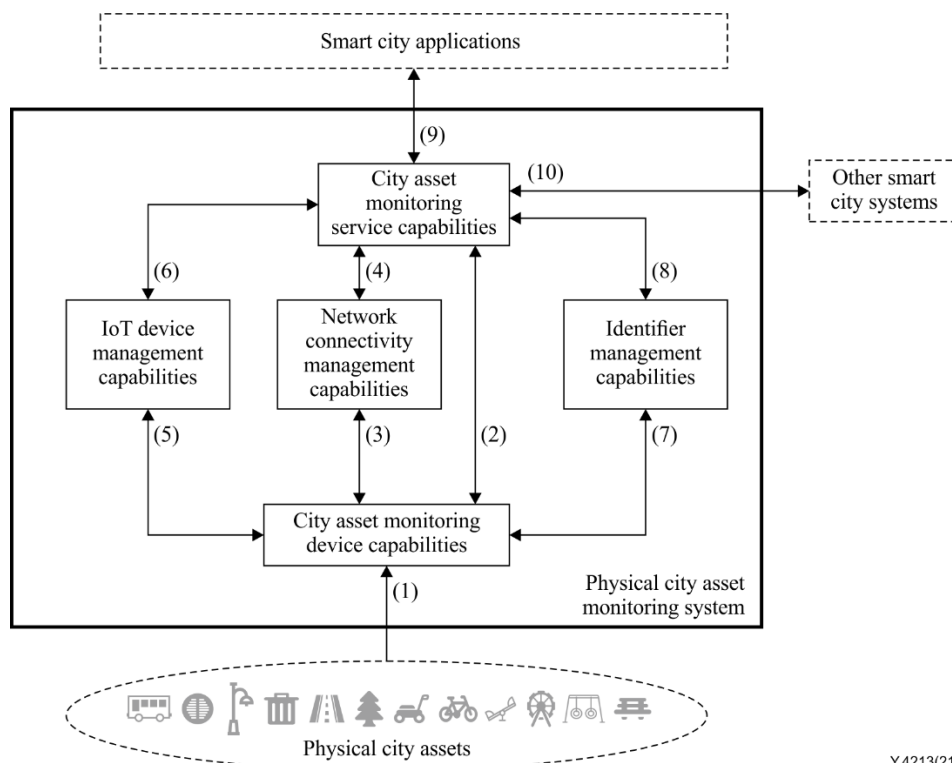
Figure 2 – Capability framework of physical city asset monitoring system

The city asset monitoring device capabilities use sensors (such as sensors of optics, gravity, electromagnetics etc.) to monitor the state of physical city assets (Figure 2, arrow (1)) and send the state to the city asset monitoring service capabilities (Figure 2, arrow (2)).

NOTE 1 – The city asset monitoring device capabilities are provided by IoT devices, which can be integrated in physical city assets (typically, streetlights, buses, waste bins and others) or deployed independently (typically, parking cameras, air sensors and others).

NOTE 2 – Examples of state attributes of physical city assets include a physical city asset's geographical position, moving or stationary condition, environmental information, etc.

The network connectivity management capabilities collect network connectivity related information, such as access network related QoS information, of the city asset monitoring devices (Figure 2, arrow (3)) and report network connectivity related information to the city asset monitoring service capabilities (Figure 2, arrow (4)).

The IoT device management capabilities, according to the commands from the city asset monitoring service capabilities (Figure 2, arrow (6)), manage the physical city asset monitoring devices (Figure 2, arrow (5)).

The identifier management capabilities handle the identifiers of city asset monitoring devices (Figure 2, arrow (7)), handle the binding of the identifiers of city asset monitoring devices with the identifiers of physical city assets and enable city asset monitoring service capabilities (Figure 2, arrow (8)).

The city asset monitoring service capabilities integrate different capabilities of the physical city asset monitoring system to enable smart city applications (Figure 2, arrow (9)). In addition, the city asset monitoring service capabilities interoperate with other smart city systems for mutual support (Figure 2, arrow (10)).

Referring to SCPs as described in [ITU-T Y.4201], Figure 3 shows the mapping to an SCP of the city asset monitoring device capabilities, network connectivity management capabilities, IoT device management capabilities, city asset monitoring service capabilities and identifier management capabilities.
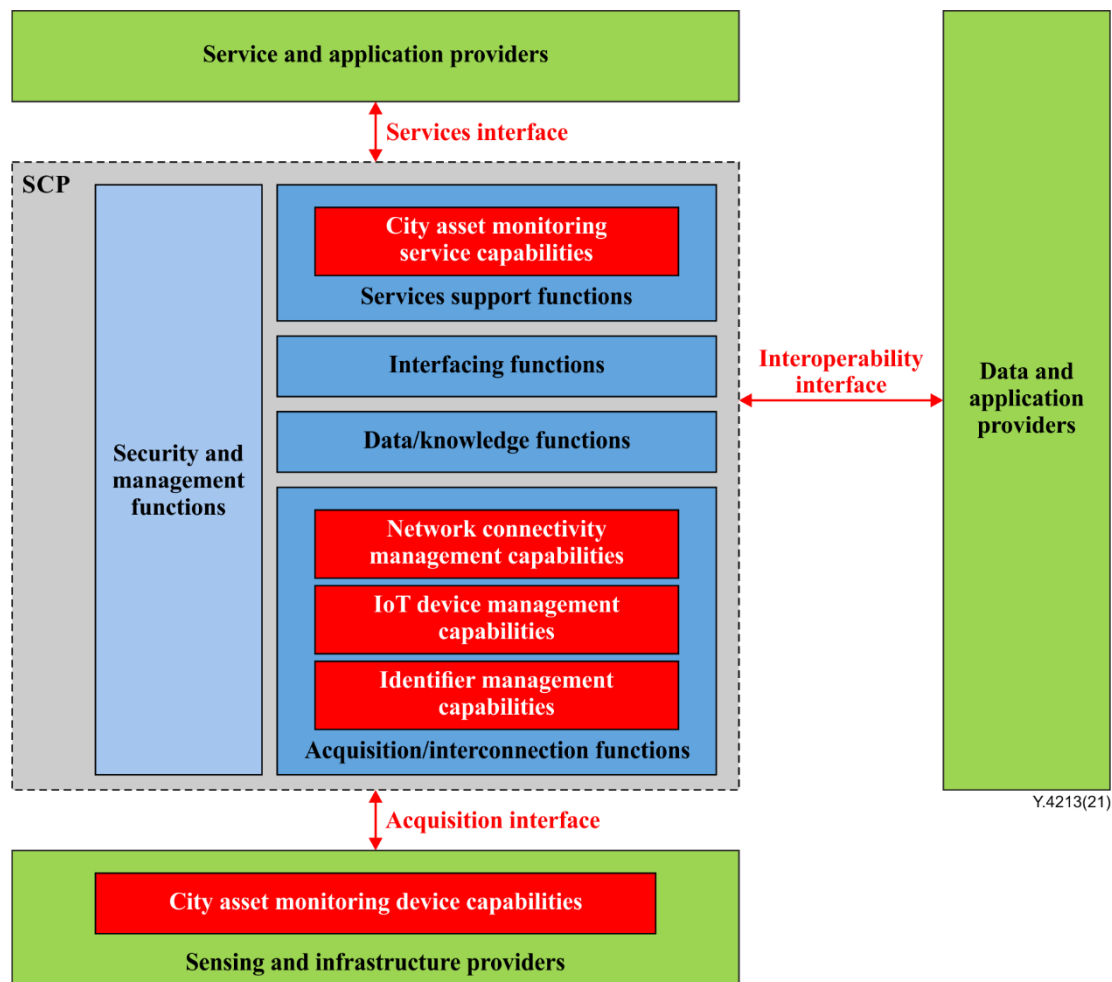
Figure 3 – Mapping of the capabilities of the physical city asset monitoring system to an SCP [ITU-T Y.4201]

8.1 City asset monitoring device capabilities

City asset monitoring devices are devices which monitor the state of the city assets.

City asset monitoring device capabilities include the following capabilities:

- Identification support;
- Locating support;
- Remote updating.

8.1.1 Identification support

In support of the requirements identified in clause 7.6, identification support capability is required. This capability enables the addition, deletion, modification and reading of the device identifier.

NOTE 1 – The device identifier is a combination of signs which can be used to identify the device.

NOTE 2 – Examples of the signs include letters, numbers and symbols.

NOTE 3 – When the identity of a device represents sensitive information, the identification support capability needs to support the creation, storage and modification of encryption keys associated with the device identifier.

8.1.2 Locating support

In support of the requirements identified in clause 7.1, locating support capability is required.

NOTE 1 – Outdoor localization technology can be used for outdoor monitoring of physical city assets. Examples of outdoor localization technology include global navigation satellite system (GNSS) and location-based services (LBS).

NOTE 2 – Indoor localization technology can be used for indoor monitoring of physical city assets. Examples of indoor localization technology include wireless fidelity (WiFi), radio frequency identification (RFID), infrared, ultrasonic technology, Bluetooth and ultra-wideband.

8.1.3 Remote updating

In support of the requirements identified in clause 7.8, remote updating capability is required. This capability enables the upgrade, rollback and pause of upgrading of the devices' software.

8.2 Network connectivity management capability

In support of the requirements identified in clauses 7.2, 7.3 and 7.4, network connectivity management capability [ITU-T Y.4212] is required. This capability enables a smart city asset monitoring system to have the necessary network bandwidth and network reliability.

8.3 IoT device management capabilities

IoT device management capabilities include the following capabilities:
- IoT device status monitoring;
- IoT device configuration;
- Remote updating support;
- Open APIs;
- Network adaptation;
- Authentication and authorization.

8.3.1 IoT device status monitoring

In support of the requirements identified in clause 7.7, IoT device status monitoring capability is required. This capability enables the collection of the data associated with the IoT device status and the reporting of the IoT device status to the city asset monitoring service capabilities.

8.3.2 IoT device configuration

In support of the requirements identified in clause 7.8, IoT device configuration capability is required. This capability enables the configuration of the city asset monitoring devices.

NOTE 1 – The IoT device configuration capability needs to support the configuring of the city asset monitoring devices in a remote way.

NOTE 2 – The IoT device configuration capability needs to support the grouping of the city asset monitoring devices and configuration of the city asset monitoring devices of a group in a batched way.

8.3.3 Remote updating support

In support of the requirements identified in clause 7.8, remote updating support capabilities is required. This capability enables firmware release, firmware update, firmware fallback, etc.

8.3.4 Open APIs

In support of the requirements identified in clause 7.5, open APIs are recommended. This enables the IoT device management capabilities to interoperate with each other in a cost efficient way.

8.3.5 Network adaptation

In support of the requirements identified in clause 7.2, network adaptation is required. This capability enables the accessibility of the IoT device management capabilities no matter what network technologies are used for network coverage.

8.3.6 Authentication and authorization

In support of the requirements identified in clause 7.5, authentication and authorization capabilities are required. These capabilities enable access control.

NOTE 1 – The authentication verifies the identity of the users who request to access the IoT device management capabilities.

NOTE 2 – The authorization grants the corresponding authority to be assigned to the users according to its authentication result.

8.4 Identifier management capabilities

Identifier management capabilities include the following capabilities:

• Identifier request;

• Identifier allocation;

• Identifier related information release.

8.4.1 Identifier request

In support of the requirements identified in clause 7.6, identifier request capabilities are recommended. These capabilities allow the physical city asset monitoring system's administrator to apply for identifiers of IoT devices which are used to monitor the physical city assets.

NOTE – Identifiers need to be provided by certified identifier providers of public identification services, in order to ensure the identifiers are globally unique.

8.4.2 Identifier allocation

In support of the requirements identified in clause 7.6, identifier allocation capabilities are recommended to have the ability to allocate identifiers to IoT devices which are used to monitor the physical city assets, according to identifier allocation rules.

NOTE – More than one identifier may be allocated to a single IoT device.

8.4.3 Identifier related information release

In support of the requirements identified in clause 7.6, identifier related information release capabilities are recommended. These capabilities enable the release of identifier related information to users according to their access rights.

8.5 City asset monitoring service capabilities

City asset monitoring service capabilities include the following capabilities:

• City asset static information provision;

• City asset status provision;

• City asset location information provision;

• Data visualization.

8.5.1 City asset static information provision

In support of the requirements identified in clause 7.5, city asset static information provision capabilities are required. These capabilities enable the provision of city asset static information (e.g., name, category, owners and usage status) to users with access control protection.

NOTE 1 – The information provided by the city asset static information provision capabilities needs to be associated with globally unique identifiers as these can help the city asset related information to be discovered and retrieved by users.

NOTE 2 – The presentation of the information provided by the city asset static information provision capabilities can benefit from the usage of semantics based technologies.

8.5.2 City asset status provision

In support of the requirements identified in clause 7.5, city asset status provision capabilities are recommended. These capabilities enable the provision of city asset status to smart city applications as well as other smart city systems according to the corresponding access rights.

NOTE 1 – Real-time status of city assets and sensitive statistical information of city asset status may be provided with access right control.

NOTE 2 – Non-sensitive statistical information of city asset status may be provided without access right control.

8.5.3 City asset location information provision

In support of the requirements identified in clauses 7.1 and 7.5, city asset location information provision capabilities are recommended. These capabilities enable the provision of location information of city assets to smart city applications as well as other smart city systems according to the corresponding access rights.

NOTE 1 – Sensitive statistical location information of city assets may be provided to users with access right control.

NOTE 2 – Non-sensitive statistical location information of city assets may be provided to users without access right control.

8.5.4 Data visualization

In support of the requirements identified in clause 7.5, data visualization capabilities are required. These capabilities enable the presentation of city asset data with multidimensional graphics and animations. Data modelling, semantics based technologies, user-friendly data description, display technologies and other data visualization related technologies may be used in support.

Bibliography

[b-ITU-T F.751.0]   Recommendation ITU-T F.751.0 (2020), *Requirements for distributed ledger systems*.

[b-ITU-T X.800]   Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b- ITU-T X.811]   Recommendation ITU-T X.811 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

[b-ISO/IEC 27000]   ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO 55000]   ISO 55000:2014, *Asset management – Overview, principles and terminology*.

[b-ISO 55001]   ISO 55001:2014, *Asset management – Management systems – Requirements*.

[b-ISO 55002]   ISO 55002:2014, *Asset management – Management systems – Guidelines for the application of ISO 55001*.

SERIES OF ITU-T RECOMMENDATIONS

Series A   Organization of the work of ITU-T

Series D   Tariff and accounting principles and international telecommunication/ICT economic and policy issues

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   Environment and ICTs, climate change, e-waste, energy efficiency; 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   Telephone transmission quality, telephone installations, local line networks

Series Q   Switching and signalling, and associated measurements and tests

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, next-generation networks, Internet of Things and smart cities

Series Z   Languages and general software aspects for telecommunication systems