International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4201

(02/2018)

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

High-level requirements and reference framework of smart city platforms

Recommendation ITU-T Y.4201

International Telecommunication Union

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
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
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.4201

High-level requirements and reference framework of smart city platforms

Summary

Recommendation ITU-T Y.4201 presents the high-level requirements and reference framework of smart city platforms (SCPs).

The SCP is a fundamental platform supporting all the services and applications of a smart city, with the objective to improve quality of life, provide urban operation and services for the benefit of citizens while ensuring city sustainability.

These high-level requirements include comprehensive and updated repositories of city information, infrastructure life-cycle management, inter-system communication, security support, maintenance support, processor controls, decision-making support, real-time dissemination of public information, resilience and interoperability.

This Recommendation benefits the plan, design, construction, deployment, operation and maintenance of smart cities and communities.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4201	2018-02-06	20	11.1002/1000/13388

Keywords

Cities, information and communication technologies (ICTs), Internet of things (IoT), smart cities and communities (SCCs), smart city platform (SCP).

* 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, 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.4201

High-level requirements and reference framework of smart city platforms

1 Scope

This Recommendation defines the reference framework and high-level requirements of smart city platforms.

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.3600] Recommendation ITU-T Y.3600 (2015), *Big data – Cloud computing based requirements and capabilities.*

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

[ITU-T Y.4900] Recommendation ITU-T Y.4900/L.1600 (2016), *Overview of key performance indicators in smart sustainable cities.*

[ITU-T Y.4903] Recommendation ITU-T Y.4903/L.1603 (2016), *Key performance indicators for smart sustainable cities to assess the achievement of sustainable development goals.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 big data [ITU-T Y.3600]: A paradigm for enabling the collection, storage, management, analysis and visualization, potentially under real-time constraints, of extensive datasets with heterogeneous characteristics.

NOTE – Examples of dataset characteristics include high-volume, high-velocity, high-variety, etc.

3.1.2 city [ITU-T Y.4900]: An urban geographical area with one (or several) local government and planning authorities.

3.1.3 open standards [b-OpenStandards]: Standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process.

NOTE – Open Standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption.

3.1.4 smart sustainable city (SSC) [ITU-T Y.4900]: A smart sustainable city is an innovative city that uses Information and Communication Technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social, environmental and cultural aspects.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 city platform: A computer system or integration of computer systems that uses information and communication technologies (ICTs) to access data sources and process them to offer urban operation and services to the city.

NOTE – The concept is extended to a community.

3.2.2 corrective maintenance: Maintenance performed after a problem occurs.

NOTE – The SCP is recommended to manage notifications or warnings and ensure technical possibilities to send messages, e-mails, SMS and make telephone calls related to these notifications and warnings.

3.2.3 open interface: A public standard for connecting hardware to hardware and software to software. Open interfaces are designed and documented for safe and easy use by third party developers and freely available to all.

3.2.4 preventive maintenance: Maintenance performed on an SCP regularly while it is still in operational order to reduce failure.

NOTE – The SCP is recommended to store and assess the relevant indicators for maintenance management. The maintenance plans should be based on these indicators.

3.2.5 smart city platform (SCP): 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.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CEP	Complex Event Processing
ETL	Extract, Transform, Load
GIS	Geographic Information System
ICT	Information and Communication Technology
IoT	Internet of Things
IT	Information Technology
JMX	Java Management extensions
M2M	Machine-to-Machine
OAM	Operation, Administration and Maintenance
REST	Representational State Transfer
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SCC	Smart Cities and Communities
SDK	Software Development Kit
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SSC	Smart Sustainable City

5 Conventions

In this Recommendation:

The expression "is required" indicates a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The expression "is recommended" indicates a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance with this Recommendation.

The expression "can optionally" and "may" indicates an optional requirement which is permissible, without implying any sense of being recommended. This term is 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 this Recommendation.

6 Overview of smart city platforms

An SCP is designed to provide means for enabling new smart city applications to be rapidly created, deployed, extended and managed. It is recommended to provide tools and services for aggregation and backhauling of data communication, city cloud architectures, IoT service creation, security and threat intelligence, device and connectivity management platforms, data collection, analytics, while also addressing customer experience.

An SCP directly integrates city platforms and systems (i.e., SCP functions), or through open interfaces between the SCP and external providers, to offer urban operation and services supporting the functioning of city services, as well as efficiency, performance, security and scalability. As illustrated in Figure 1, an SCP has the following SCP functions:

– services support functions,
– interfacing functions,
– data/knowledge functions,
– acquisition/interconnection functions, and
– security and management functions.

The external providers include:

– services and applications providers,
– data and computation providers, and
– sensing and infrastructure providers.

There are interfaces for communication between the SCP with the external systems or other platforms. These interfaces are shown in Figure 1 as red arrows and are detailed in the following list:

– The services interface connects an SCP's services support functions and the external data and computation providers.
– The interoperability interface connects an SCP's data/knowledge functions interoperability and the external database and computation systems.
– The acquisition interface connects an SCP's acquisition/interconnection functions and the external sensing and infrastructure systems.

All the above interfaces are required to implement open standards.

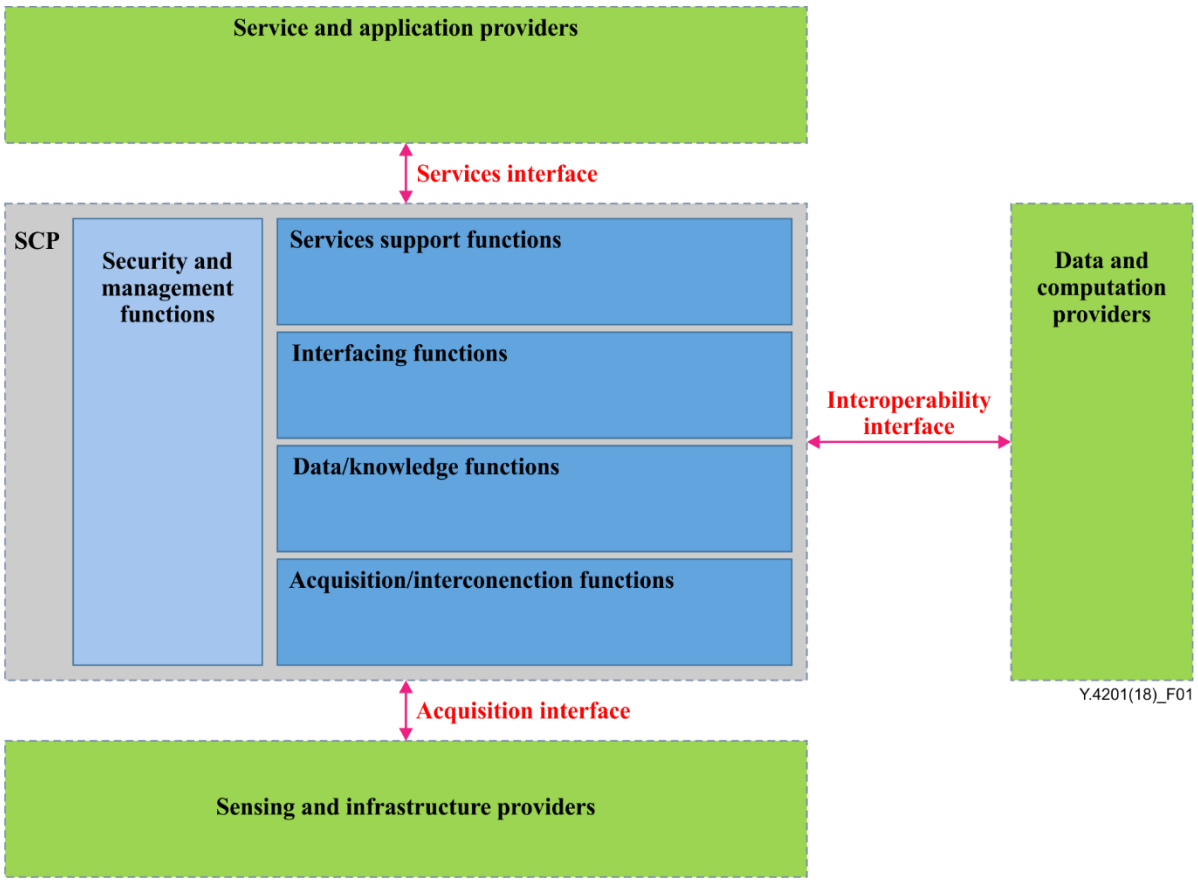

Figure 1 – Overview of an SCP and external systems/platforms

6.1 SCP functionalities

The SCP is required to enable the integration of existing and future city applications and services.

The SCP is required to allow city managers to:

a) manage the city's infrastructure including remote provisioning, configuration, firmware updates and device troubleshooting;

b) make decisions based on the data received and processed;

c) coordinate services (e.g., emergency services);

d) control service quality;

e) showcase the status of the city's infrastructure and services;

f) log city events;

g) distribute relevant data and information to citizens;

h) support the reuse of applications, devices and network infrastructure;

i) connect the city platform with different vertical systems;

j) interconnect the city platform with other city platforms;

k) provide reference points to connect the city platform with external third-party services;

l) protect smart city assets and prevent infections via security analytics and threat intelligence.

The SCP may enable scenario simulations, forecasting and planning.

6.2 General principles of building SCPs

The following general principles of building SCPs are required to be met.

a) Horizontality: support capabilities in different fields of application, enabling the simultaneous deployment of multiple services on the same infrastructure.

b) Interoperability: capability of supporting different technologies for capturing information, and open standards, as well as interconnecting with internal/corporate and/or external information systems. This feature is described in detail in [ITU-T Y.4200].

c) Performance: ability to handle a large number of devices, services and processes efficiently.

d) Scalability: ability to increase processing, interconnecting and storage capacities without needing to change the architecture.

e) Robustness and resilience: capability to continue to function when faced with problems.

f) Security: guarantee of data preservation and reliability.

g) Modularity: ability to be easily broken down into parts.

h) Flexibility: applicability to various smart city services.

i) Extensibility: growth capability to meet new needs.

j) Semantics: ability to develop the data structures containing the meaning of concepts, properties, and relationships that formally represent city entities, events and scenes.

k) Based on open standards: simplifying the integration with other platforms and developing applications on the platform that may be reused and portable among different platforms.

l) Operable and manageable: provide tools for installing, operating, managing and maintaining the platform.

7 High-level requirements of SCPs

7.1 Comprehensive and updated repository of city information

The SCP is required to handle a comprehensive and updated repository of city information through the following functions:

a) hosting a freely accessible catalogue of standardized data on the city;

c) enabling cross-city overviews using this data;

d) facilitating the integration of data with varying levels of latency;

e) providing open and standardized interfaces for external providers to access this data;

f) enabling security and integrity of data, as well as security of users.

7.2 Infrastructure life-cycle management

The SCP is required to coordinate the management of the infrastructure, considering secure and multi-user monitoring and operation of different city resources, elements or systems. The SCP is required to orchestrate the sensing and infrastructure providers, for instance, public transportation systems, energy production, waste collection, off-street and on-street parking management, etc. via the acquisition interface (see Figure 1). The external management of infrastructure includes:

a) access to data from sensors, databases and information from other applications;

b) the operation of city sensors using standardized solutions;

c) registration of different activities carried out on city resources, elements or systems;

d) management of maintenance of equipment and infrastructure;

e) support monitoring tools such as Java management extensions (JMX) or monitoring protocols such as the simple network management protocol (SNMP).

7.3 Inter-system communications

The SCP is required to allow inter-system communications through the following functions:

a) use open and secure application programming interfaces (APIs) and standard protocols to communicate between applications and with other management systems;

b) conditional and secure access to emergency services.

7.4 Security support

7.4.1 General aspects

The SCP is required to include appropriate measures to maximize privacy and security of citizens by implementing tools in order to:

a) Back up critical information.

b) Guarantee non-repudiation in network security.

c) Support anonymised data.

d) Guarantee security and integrity of data.

e) Support authentication and authorisation.

f) Control access to the platform and to all the elements accessed through it.

g) Support confidential communications.

h) Ensure confidential access to data, ensuring that each agent only has access rights to the data assigned to it.

i) Define and manage security policies.

j) Maintain repositories of existing users registered by local authorities.

7.4.2 Profiling

The SCP is recommended to ensure the privacy or security of the data stored or managed by the city, particularly in environments with shared resources. Furthermore, different access profiles can access different types of groups of data, thereby avoiding their misuse.

The SCP is recommended to guarantee the secure exchange of data along the platform from the physical devices to applications.

The SCP is recommended to allow for the definition of different profiles (such as administrator, external providers, citizens) with appropriate access rights, authorising or denying access to the different applications and defining the required privileges for operating with identified sets of data.

Management of roles/permissions is recommended to be established at least for three security levels:

a) Data access: limiting the information that can be viewed by each user. For example, a user of a specific service only has access to information corresponding to its service.

b) Access to the elements of the platform: limit access to reports and dashboards configured in the platform. For example, a user of a service is only able to access reports defined by the data corresponding to their role.

c) Functions: limited actions available to a certain user according to their profile. For example, a user of a report may determine which reports or objects final users have access to.

7.5 Maintenance support

The SCP is required to include appropriate measures for its adequate maintenance.

The SCP is recommended to support preventive maintenance and corrective maintenance.

7.6 Showcase support

The SCP is required to include the functionality of showcasing the status of its infrastructure and services. The presence of information includes:

a) **Status of city infrastructure**:

- engineering infrastructures, such as energy supply, water supply and drainage, transportation, logistics, communication, environment and disaster prevention;
- social infrastructure, such as administration, welfare, health, education, science, culture, sports, and entertainment.

b) **Information of services** [ITU-T Y.4903]:

- economy aspects, such as employment, trade, productivity and innovation;
- environmental aspects, such as air quality, water and sanitation, noise, soil and biodiversity;
- societal and cultural aspects, such as education, health, safety, housing and culture.

7.7 Controls of processes

It is recommended that the SCP supports controlling the following internal and/or external processes:

– consumption analysis, warnings and trends, etc.;

– cost allocation;

– sustainability (efficient use of facilities, greenhouse gas emissions, etc.) and reliability of infrastructures;

– optimization of processes and planning;

– crisis dashboard.

The SCP is also recommended to support the generation of operating reports.

7.8 Support for decision making

The SCP is recommended to support decision-making processes to improve city resilience by providing:

– simulations based on current and past information;

– assessment and deployment of action plans in complex scenarios;

– predictive modelled analysis of the city;

– data mining and statistical analysis;

– integration with business intelligence systems and tools.

7.9 Real time dissemination of public information

The SCP is required to enable transmission of open, reliable and quality information, on a constant basis and free from interruptions, in standardized formats to be accessible from multiple ICT devices.

This information is applicable to the following scenarios:

– end-user citizen services (the information society);

– external services and applications;

– other administrative public services;

– services for purposes of accountability (transparency).

7.10 Resiliency

The SCP is recommended to:

– Ensure the ongoing operation of services according to established service level agreements (SLAs). These services may require availability 24X7 and a service level of over 99.9% annually. Providers may offer solutions complying with these requirements.

– Guarantee disaster recovery with limited recovery time objectives (RTOs) and recovery point objectives (RPOs).

7.11 Interoperability

The SCP is required to comply with [ITU-T Y.4200].

8 Reference framework of SCP

8.1 Architecture of SCPs

The architecture of an SCP (shown in Figure 1) can be described in detail (shown in Figure 2). Each function offers capabilities; these are detailed below:

– Acquisition/interconnection functions: offer mechanisms for capturing data from the collection systems (see clause 8.2). They also enable interconnection with other external providers that only use data. These functions provide other capabilities such as:

  • Abstract: This allows for the gathering and refining of data from devices for desired processing in an agnostic manner.

  • Tagging: This allows for the received information to be transformed to the data structures defined in the platform. It allows for the source of the data received to be identified by adding tags including identifier and registration information.

– Data/knowledge functions: support the processing of data (see clause 8.3). They receive data from both the acquisition/interconnection functions and the interfacing functions and include functionalities which enable the movement of large amounts of data, and data processing and analysis functionalities to generate new datasets or modify/complete existing ones. Other functionalities offered are:

  • Data management: This provides a systematic way to create, retrieve, update and manage data.

  • Data analysis: This provides the capacity to analyse the data.

  • Big data: This provides the capacity to store and work with large amounts of data.

  • Geographic information system (GIS): This provides the capacity to work with geospatial information.

  • Real-time repository: This provides the capacity to work with information in real time.

– Interfacing functions: provision of services for smart cities (see clause 8.4). They also offer open and standardized interfaces for the data/knowledge functions and the services support functions, which are compliant with the security policies. Other functionalities that are provided are:

  • APIs that allow access to the service provided by the SCP.

  • Open data portal that allows data to be made publicly available.

– Services support functions: These support various services connected through interfacing functions and the APIs supplied (see clause 8.5). Applications can be running on the platform or can be other external services that publish or use the information. Some services support functions that may be offered are:

- e-Government support: These services are enabled to match electronic public administration and other government needs.
- Transportation support: These services manage transport information and allow the traffic of the city to be managed.

– Security and management functions: These functions provide horizontal support to the other functions by offering services such as audits, monitoring and security (see clause 8.6). Some of the functions that may be offered are:

- Security: This provides security mechanisms such as authentication, authorization, ciphering, etc.
- Monitoring: This collects platform operation information.
- Audit: This registers who has accessed sensitive information.
- Logging: This traces the execution of the applications and/or the systems of the platform.
- Configuration: This allows access to the configuration of the systems and to change the execution parameters.
- Operation, administration and maintenance (OAM): Processes and tools that allow the platform to be operated, managed and maintained.

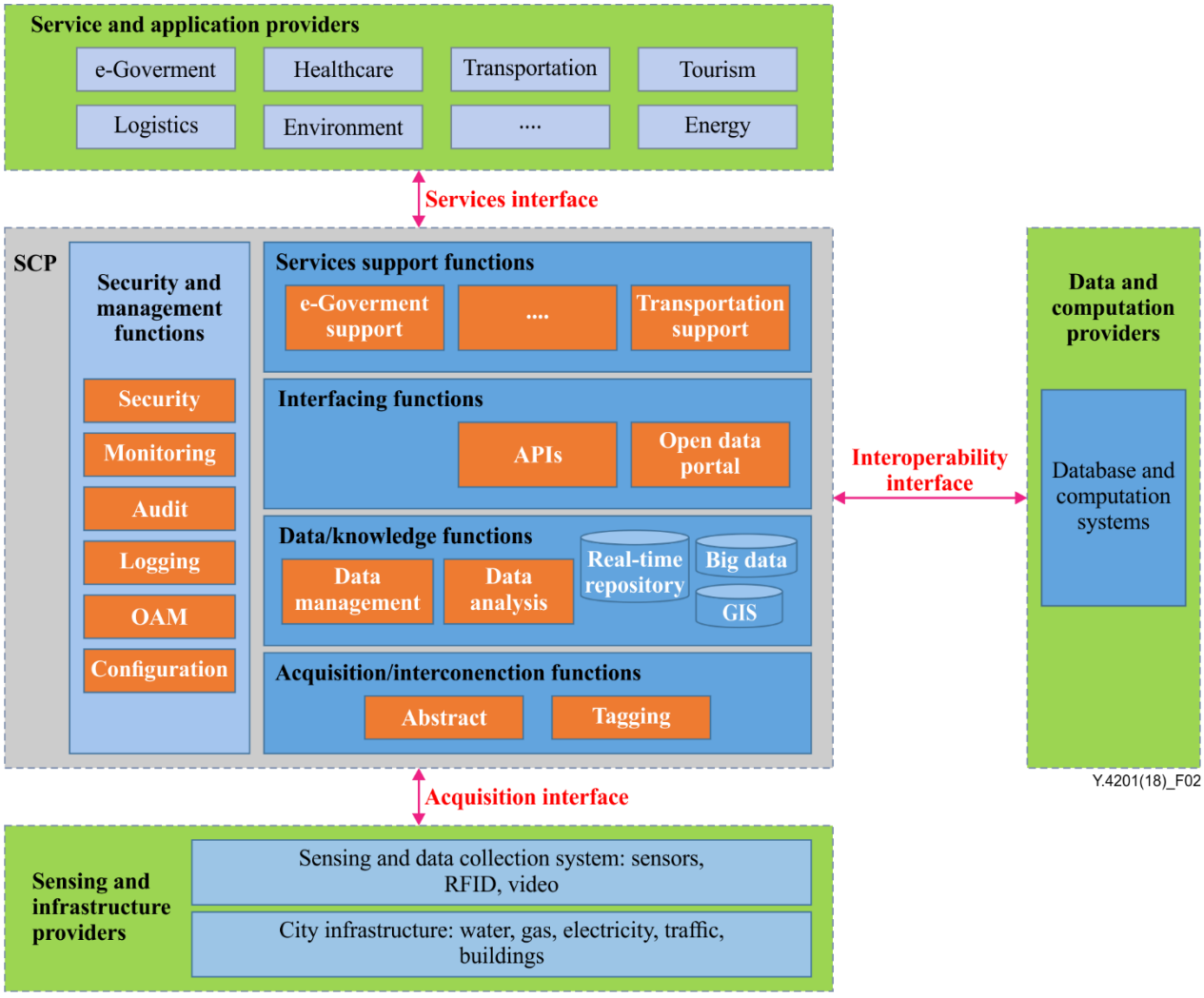

Figure 2 – Reference framework of an SCP

8.2 Acquisition/interconnection functions

It is required that the acquisition/interconnection functions:

a) Integrate information from the different sources of data (collection systems) as defined in [ITU-T Y.4200] that may include:
   - sensors, actuators, gateways and devices such as traffic lights, buildings, weather stations;
   - personal mobile devices, vehicles or digital home devices;
   - social networks;
   - other information technology (IT) systems, such as SCADAs or vertical domain management solutions, which may be proprietary solutions.

b) Supply information to the data/knowledge functions independently from the devices, and formatting the acquired data according to semantic processing.

c) The acquisition/interconnection functions are independent of network information and control.

The acquisition/interconnection functions are required to support:

– independent end-to-end services for accessing devices;

– interfaces, APIs and open standard protocols;

– security and monitoring;

– discovery and access to IoT/machine-to-machine (M2M) applications;

– identification and naming of devices and applications; and

– management aspects (including remote management of entities).

8.3 Data/knowledge functions

The data/knowledge functions contain elements for processing, managing and using information.

It is required that the data/knowledge functions handle:

a) integration of information from the external systems and computation systems as defined in [ITU-T Y.4200];

b) access to all information (both past records and real-time information);

c) movement of data received from the acquisition/interconnection functions, between the different functions of the knowledge functions for storage, processing and recovery, and towards the interfacing functions. Data in these functions has already been extracted from the source devices and is recommended to be processed following standard data models;

d) support for real-time processing of data received from the acquisition/interconnection functions through modules with complex event processing (CEP) engines, rule engines;

e) batch handling support for data received from extract, transform, load (ETL) and machine learning;

f) support for analytical processing of data using business intelligence processes, etc;

g) support for GIS processing of data to enable geolocation, carrying out geographical queries;

h) security in data access, to control which user/role/profile is accessing which data.

The data/knowledge functions are recommended to include components to enable the semantic processing of data, including data management and data analysis.

8.4 Interfacing functions

The interfacing functions facilitate the provision of services for smart cities by offering interfaces and functions, such as the development kit and web portal that will be used to implement the services rendered to clients, such as:

– interconnection between applications and platforms;

– access to the platform by external services;

– publishing of an open data portal that can be used from the services support functions;

– building services inside the service support functions using the development kit that includes software development kits (SDKs);

– secure access to the APIs, the development kit, web portal, etc.

Portability between platforms and cities is recommended to be guaranteed based on a set of standard APIs in the interfacing functions, thereby creating a real ecosystem of applications with a critical mass that lowers the access barrier to developers of applications.

The APIs are required to follow the overall API representational state transfer (REST) trend.

The APIs are recommended to support different data access modes, including push (subscription and notification) and pull (request and response). They are also recommended to support geo-referenced queries.

The API data access model may not distinguish between the specific data models, but in order to ensure interoperability, it is recommended to use a means of transport that is compatible with the existing data model.

8.5 Services support functions

The services support functions provide support to municipal services and business and value added applications by:

a) support of the external services and applications as defined in [ITU-T Y.4200];

b) command centres deployed depending on user's profiles and permissions;

c) integrated maintenance contract management application, including SLAs based on real data.

These services and applications, such as e-government, healthcare, transportation, tourism, logistics, environment and energy management, can be developed by external providers. Therefore, it is required that this function enables the deployment of these services in the SCP. Services developed by external providers can access all information and the services offered by the platform through interfacing functions.

8.6 Security and management functions

These functions provide horizontal support to the other functions by offering services such as security, monitoring, audits, logging, OAM, configuration, etc., including:

a) configuration of a platform repository to allow storage of all configuration information;

b) online configuration management enabling overall management using an online application including API REST management interfaces;

c) security repository connectors enabling platform security to be delegated to the city's user management solution.

Bibliography

[b-OpenStandards] *Definition of Open Standards*, http://www.itu.int/en/ITU-T/ipr/Pages/open.aspx.

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

Printed in Switzerland
Geneva, 2018