MCMC MTSFB TC Gxxx:2023

TECHNICAL CODE

INTEROPERABILITY REQUIREMENTS FOR SMART CITY PLATFORMS

Developed by

Registered by

Registered date:

MCMC MTSFB TC Gxxx:2023

Development of technical codes

The Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) (‘the Act’) provides for a Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission (‘the Commission’) to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirements for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd (‘MTSFB’) as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
http://www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
MCMC Tower 2
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8680 9950
Fax: +60 3 8680 9940
http://www.mtsfb.org.my

Contents

Page

Committee representation

This technical code was developed by the Internet of Things and Smart Sustainable Cities Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB), which consists of representatives from the following organisations:

CelcomDigi Berhad

Cyberview Sdn Bhd

Favoriot Sdn Bhd

Heriot-Watt University Malaysia

Kiwitech Sdn. Bhd.

Maxis Broadband Sdn Bhd

SIRIM Berhad

Sunway University College Sdn Bhd

TM Technology Services Sdn Bhd

UCSI Education Sdn Bhd

Universiti Malaya

Universiti Putra Malaysia

Universiti Teknologi MARA

Foreword

This technical code for Interoperability Requirements for Smart city Platforms ('Technical Code') was developed pursuant to Section 185 of the Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) by the Internet of Things and Smart Sustainable Cities Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB).

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

INTEROPERABILITY REQUIREMENTS FOR SMART CITY PLATFORMS

0. Introduction

Cities and communities face a growing need to deliver services while minimizing costs, necessitating access to various data sources. In a city context, systems can be categorized as internal systems, encompassing traditional community services like waste management, lighting, parking, and traffic control, among others. External systems include transportation companies, ports, airports, buildings, hotels, and social networks. These systems possess valuable information about the city's state and can be managed using diverse control tools such as IoT platforms, Supervisory Control and Data Acquisition (SCADA) systems, non-IoT platforms, and big data processors. However, these control tools often operate independently, lack standardization, and hinder resource and data sharing.

To address this challenge, a Smart City Platform (SCP) should have the capability to access multiple information sources, facilitate resource sharing, analyse capacity, and coordinate services, typically through predictive analysis. The concept of horizontality is crucial in SCP implementation, as it promotes the interaction of information from various sources to deliver specific services instead of relying solely on its own sensors.

The applications of SCPs are wide-ranging, spanning from emergency traffic control to proactive demand management in museums due to unexpected tourist influxes.

This Technical Code outlines the requirements for SCP interoperability and serves as a reference point to ensure the seamless functioning of city services.

1. Scope

This technical code establishes the necessary criteria for achieving interoperability among SCPs and their reference points, thus ensuring the proper operation of city services.

The SCP plays a vital role in delivering services within a smart city. Interoperability between SCPs facilitates the expansion of service offerings and improves their quality. It enables the provision of enhanced services to citizens while ensuring maximum efficiency, scalability, and seamless integration.

Moreover, by enabling interoperability with other platforms, the SCP fosters local economic development by promoting innovation and competition. This encourages the growth of new solutions and advancements within the smart city ecosystem.

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

MCMC MTSFB TC T007:2020, *Short Range Devices (SRD) – Specifications (Second Revision)*

MCMC MTFSB TC T012: 2015, *Specification for Land Mobile Radio Equipment*

MCMC MTSFB TC T018:2021, *Global System for Mobile Communications and Long Term Evolution – Cellular Booster Equipment*

MCMC MTSFB TC T015:2022, *IMT Advanced (Long Term Evolution) – User Equipment (First Revision)*

ISO/IEC 8824, *Information technology: Abstract Syntax Notation One (ASN.1)*

ISO/IEC 20922, *Information technology: Message Queuing Telemetry Transport (MQTT)*

ISO/IEC 21778, *Information technology - The JSON data interchange syntax*

Malaysia Government Enterprise Architecture (MyGovEA), September 2018, *Public Sector Reference Model*

RFC 7252, *The Constrained Application Protocol (CoAP)*

TM Forum, *Open Digital Architecture (ODA) v2.0.1*

3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

API	Application Programming Interface
ASN.1	Abstract Syntax Notation One
CoAP	Constrained Application Protocol
HTTP	Hypertext Transport Protocol
ICT	Information and Communications Technology
GSMA	Global Systems for Mobile Communications
IoT	Internet of Things
JSON	JavaScript Object Notation
M2M	Machine to Machine
MQTT	Message Queuing Telemetry Transport
REST	Representational State Transfer
SCADA	Supervisory Control and Data Acquisition
SCP	Smart City Platform
SSC	Smart Sustainable City
TCP/IP	Transmission Control Protocol/Internet Protocol
XML	eXtensible Markup Language

4. Terms and definitions

For the purposes of this Technical Code, the following terms and definitions apply.

4.1 Interoperability

Ability for two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

4.2 Internet of Things (IoT)

A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving, interoperable Information and Communications Technologies (ICT).

NOTES:

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

2. In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

4.3 Open interface

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

4.4 Open standards

Publicly accessible standards developed or approved and maintained through a collaborative, consensus-driven process.

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

4.5 Policy and governance interoperability

A compatibility and alignment of policies, regulations, and governance frameworks across different entities, organizations, or jurisdictions applicable to the participating IoT systems.

NOTES: IoT device, IoT gateway, sensor and actuators are considered as an IoT system.

4.6 Semantic interoperability

It refers to interoperability where the meaning of the data model within the context of a subject area is understood by the participating IoT systems.

NOTES: IoT device, IoT gateway, sensor and actuators are considered as an IoT system.

4.7 Syntactic interoperability

It refers to interoperability where the formats of the exchanged information can be understood by the participating IoT systems.

NOTES: IoT device, IoT gateway, sensor and actuators are considered as an IoT system.

4.8 Smart City Platform (SCP)

A city platform that provides seamless integration with city systems, whether through direct interfacing or open interfaces for collaboration with third-party entities. This platform enhances urban operations and services, promoting the functionality of city services while prioritising efficiency, performance, security, and scalability.

4.9 Smart Sustainable City (SSC)

An innovative city that uses ICT 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 and environmental, as well as cultural aspects.

4.10 Transport interoperability

It refers to interoperability where information exchange uses an established communication infrastructure between the participating IoT systems.

NOTES: IoT device, IoT gateway, sensor and actuators are considered as an IoT system.

5. Overview of Internet of Things (IoT) Interoperability

The purpose of this document is to establish a shared understanding among stakeholders involved in the IoT regarding SCP interoperability tailored to their specific requirements. This shared understanding serves as a foundation for achieving interoperability in IoT by defining common terminology and concepts used to describe it, particularly in relation to SCP entities. By aligning their understanding, the involved parties can collaborate effectively towards ensuring seamless interoperability within the IoT ecosystem.

5.1 Considerations for Internet of Things (IoT) Interoperability

Interoperability can be described as the extent to which various systems or components are able to interact successfully. In the context of this Technical Code, interoperability is specifically defined in 4.1.

In the realm of the IoT, interoperability encompasses different types of entities and their associated interfaces that interact with one another. When addressing IoT interoperability, there are several key considerations, including but not limited to the following.

a) Enabling effective communication among entities existing in different domains or disparate IoT systems.

b) Facilitating the exchange of data between entities across varying domains or within different IoT systems.

c) Establishing a shared understanding of the meaning and interpretation of exchanged data, even when dealing with entities from divergent domains or separate IoT systems.

d) Providing the capability for seamless integration and collaborative interaction between different IoT services.

e) Defining the roles and functions of functional components that contribute to the efficient operation of interoperability.

By taking these into careful consideration, this Technical Code constructs a contextual framework aimed at enhancing the comprehension of both current and future interoperability standards within the realm of SCP. It stands as a valuable resource for gaining insights into the intricacies and prerequisites associated with SCP interoperability.

5.2 Internet of Things (IoT) interoperability model

5.2.1 General

Interoperability encompasses a range of factors, commencing with the straightforward exchange of data bytes, enabling an interpretation of the meaning behind the exchanged information, and fostering alignment in terms of business processes, behaviors, and policies on both ends of the interaction.

When dealing with diverse interactions that require interoperability in the realm of IoT, it becomes imperative to delve into the technological, informational, and human dimensions. Looking ahead, challenges associated with interoperability are poised to escalate and become increasingly intricate as IoT systems evolve into more intricate and interconnected entities. In IoT ecosystems, where virtually everything can be connected, intricacies extend beyond technological aspects to encompass global policies, regulations, and international laws.

Within the IoT interoperability context, four key facets are elaborated upon in the 5.2.2 until 5.2.5.

5.2.2 Transport interoperability

Transport interoperability refers to the shared communication infrastructure designed for the purpose of data exchange between different entities. This encompasses both the physical mediums employed (such as wired or wireless connections) and the mechanisms of data transport between various components within an IoT system or across disparate IoT systems. Notable examples consist of IEEE 802.3 (Ethernet), IEEE 802.11 (Wi-Fi) and Global Systems for Mobile Communications (GSMA) wireless mobile such as 4G and 5G, in addition to protocols like Transmission Control Protocol/Internet Protocol (TCP/IP), HTTP/S, Message Queuing Telemetry Transport (MQTT) (as detailed in ISO/IEC 20922), and Constrained Application Protocol (CoAP) (as outlined in RFC 7252).

5.2.3 Syntactic interoperability

Syntactic interoperability refers to the capability of two or more systems or devices to communicate by adhering to shared syntax rules, encompassing formats, protocols, and other syntactic elements. Illustrative syntaxes for data exchange encompass standards such as the Web Ontology Language (WOL), eXtensible Markup Language (XML), JavaScript Object Notation (JSON) (as delineated in ISO/IEC 21778), Abstract Syntax Notation One (ASN.1) (as detailed in the ISO/IEC 8824 series), and more.

5.2.4 Semantic interoperability

In an IoT system, domain concepts exhibit diversity and are contingent on the characteristics of the entities involved. The foundation of semantic interoperability rests on the data models employed during the data exchange process. These data models encapsulate the inherent nature of the entities in question and the functional capabilities of the interfaces linking them.

5.2.5 Policy and governance interoperability

Policy interoperability can be delineated as the capability of two or more systems to harmonize their operations within the boundaries set by the applicable legal, organisational, and policy framework governing these participating IoT systems. This facet encompasses a spectrum of considerations, including governmental laws and regulations, policy terms and conditions applicable to IoT users or providers, and the organisational policies that oversee their interactions.

The specifications related to smart city should be referred to MCMC MTSFB TC T007, MCMC MTSFB TC T018, MCMC MTSFB TC T015, MCMC MTFSB TC T012 and MyGovEA.

6. Platforms and services

The IoT platform is encompassed within the broader SCP, and the full spectrum of interoperability features detailed in Clause 5 are indeed relevant to the SCP as a whole. However, it's worth noting that the scope of this document is primarily centered on acquisition, services, and interoperability with external systems.

The current landscape of SCP is characterised by numerous vertical solutions, each implemented independently, which often presents challenges in exchanging data between these solutions. To address this issue, Figure 1 illustrates an example of how interoperability can be achieved in a SCP through the utilisation of open interfaces.

In this scenario, initially, these platforms operate independently, with each of them providing distinct services to the city. They collect data from sensors and other sources, process it, and deliver services based solely on the data they have gathered. These vertical platforms operate in isolation, not sharing information, and each manages its own systems and resources.

However, the introduction of a SCP in this context brings about a transformation. It fosters the integration and optimisation of these vertical platforms and facilitates the exchange of information and resources among them. On one hand, resources and systems employed by the vertical platforms with similar functions can be consolidated. On the other hand, the data stored and processed by one vertical platform becomes accessible to others, enabling the creation of more cost-effective, valuable, and complex services.

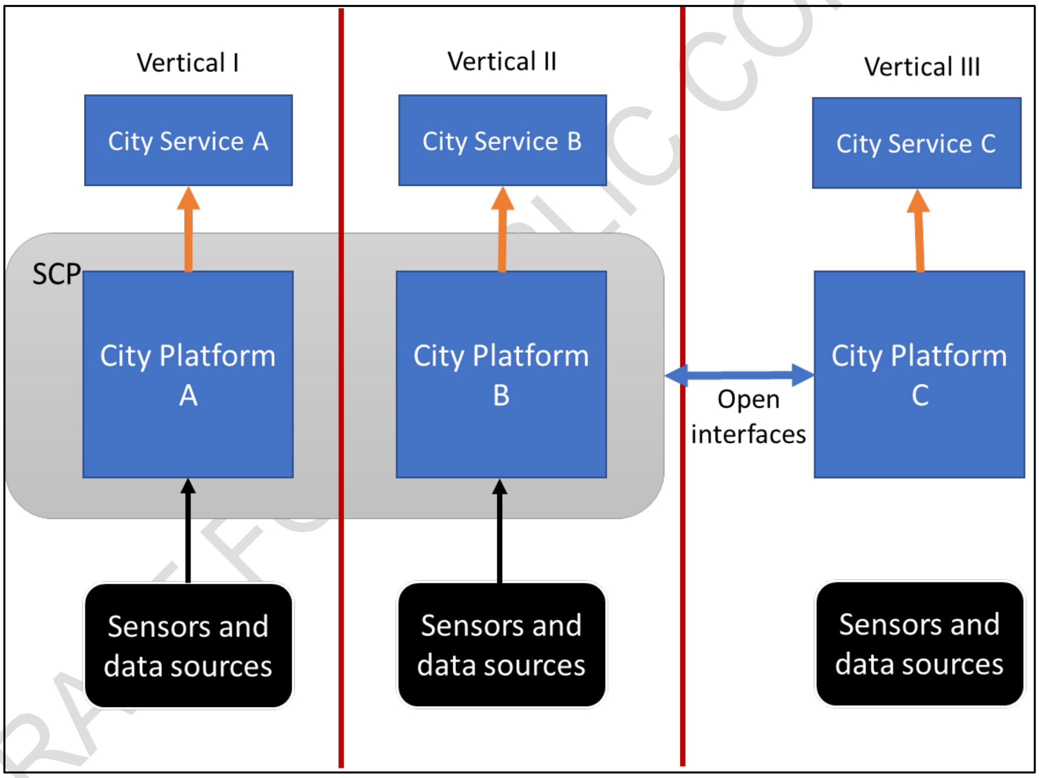

Figure 1. Smart City Platform (SCP) interactions

Figure 1 illustrates the construction of the SCP by seamlessly integrating platforms A and B. Notably, city platform C remains external to the SCP, necessitating the implementation of open interfaces for establishing connections between the SCP and city platform C. This approach serves to enhance the interoperability of the SCP with various systems and platforms, fostering more efficient collaboration.

During this integration process, certain resources, such as data sources, can be shared among the involved platforms. The broader accessibility to data sources empowers services to tap into a more extensive pool of information, potentially leading to the creation of novel services and the enhancement of existing ones. Moreover, the availability of diverse data sources facilitates predictive analysis, further broadening the possibilities for data-driven insights.

The SCP could interoperate with external providers' city platforms, and its interfaces are required to be adapted. The adaptation of these interfaces will depend on the type of platform.

An example of open architecture is the TM Forum Open Digital Architecture (ODA).

7. Smart City Platform interoperability

7.1 General description

In the context of SCP, interoperability between SCP entities is achieved when one SCP entity can successfully connect to and interact with another SCP entity. For an SCP entity to establish a connection and utilize another SCP entity, it is essential for using SCP entity to possess knowledge about the target SCP entity. This knowledge can be acquired through various mean as follows.

a) Discovery Protocol

Utilising a discovery protocol allows the SCP entity to discover and obtain information about the target SCP entity automatically.

b) Registry Service

Accessing a registry service enables the SCP entity to retrieve information about the target SCP entity from a centralised repository.

c) Manual Configuration

Alternatively, the SCP entity can be manually configured with static information about the target SCP entity that is already known.

The necessary knowledge about the target SCP entity includes specific details about the endpoint exposed by the target entity and the interface offered by that endpoint. This information encompasses but not limited to the following.

a) Transport information

This includes details about the physical layer and the protocol used for communication.

b) Syntactic structure

It involves understanding the format and structure of the exchanged data.

c) Semantic meaning

It relates to comprehending the semantic interpretation and significance of the exchanged data.

d) Behavioural aspects

This pertains to the expected behaviour and operations of the SCP entity for each interface.

e) Policy and governance

It encompasses any policies or rules that apply to the usage of the SCP entity.

Collectively, this information about interacting with an SCP entity is referred to as SCP entity metadata. Consequently, models are required to describe and define the SCP entity metadata, focusing on the endpoints and interfaces of SCP entities. These models provide a standardised representation and understanding of the necessary details for successful interoperability between SCP entities.

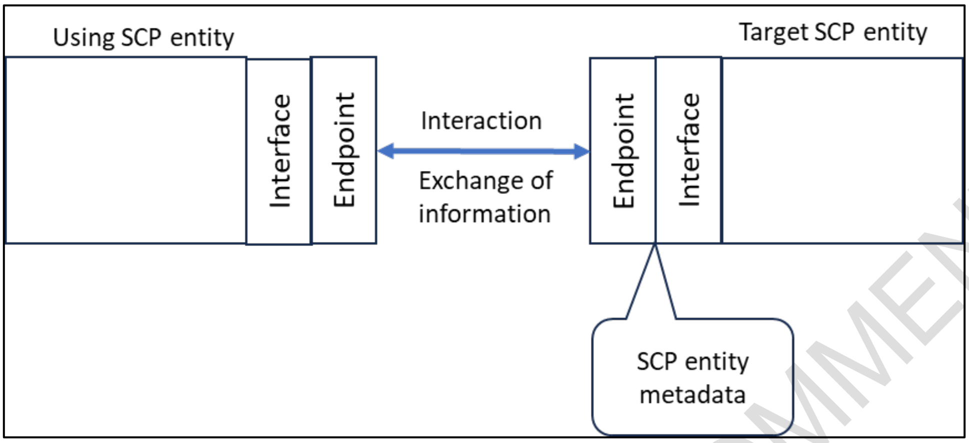

Figure 2. Concepts for interoperability of Smart City Platform (SCP) entities

Figure 2 illustrates the fundamental concepts for achieving interoperability of SCP entities. The figure depicts the interaction between two SCP entities, where information is exchanged between them. The target SCP entity provides an endpoint with an associated interface that is invoked by the using SCP entity. In order to ensure successful interoperability, it is crucial that the processes or activities of the interacting entities align harmoniously. If there is a lack of behavioural interoperability, the target entity may not be able to deliver the expected features and functionalities anticipated by the source entity.

A noteworthy aspect of any SCP entity is its potential to have multiple distinct interfaces, often exposed on different endpoints. It is common for an SCP entity to possess a functional interface that offers the primary capabilities of the entity, as well as a separate management interface that enables the entity to be effectively managed and controlled.

By acknowledging these concepts, the interoperability of SCP entities can be effectively achieved, enabling seamless communication, information exchange, and the fulfilment of desired functionalities between interacting entities.

The SCP should promote open and equitable access to data, fostering collaboration among various stakeholders, and facilitating the seamless exchange of information while adhering to data privacy, governance and security standards. The service provider must provide a disclaimer to explicitly declare data ownership.

7.2 Interoperability framework for Smart City Platform (SCP)

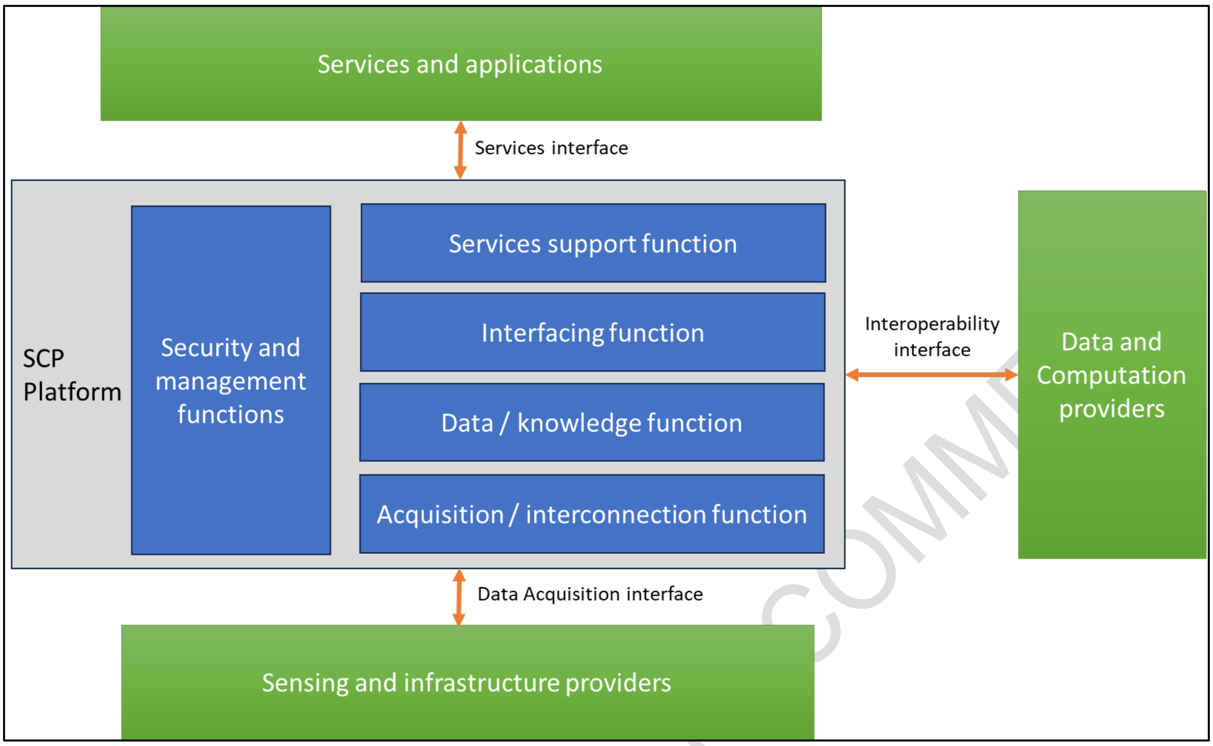
Services and applications
Services interface
SCP Platform
Security and management functions
Services support function
Interfacing function
Data / knowledge function
Acquisition / interconnection function
Interoperability interface
Data and Computation providers
Data Acquisition interface
Sensing and infrastructure providers

Figure 3. Overview of a Smart City Platform (SCP) and external systems or platforms

Figure 3 describes the architecture of an SCP and its communication with other elements. The SCP provides the following group of functions.

a) Acquisition or interconnection functions

Encompasses a set of mechanisms designed to streamline the process of obtaining data from a diverse array of collection systems. These functions play a pivotal role in ensuring that data can be efficiently and effectively captured, aggregated, and made available for further processing and analysis.

b) Data/Knowledge functions

These functions aid in the processing of data, enhancing its value and converting raw information into knowledge.

c) Interfacing functions

Interfacing functions within a system play a crucial role in ensuring that information can be accessed and utilised effectively across various levels of the organisation or platform. These functions serve as the bridge that enables communication and interaction between different components, systems, or entities, facilitating the flow of information and data.

d) Service support functions

Coordinate and manage the various services involved in actions or processes that are developed through interoperability functions. These functions help ensure that services are seamlessly delivered, monitored, and optimized for maximum efficiency and effectiveness.

e) Security and management function

Deliver horizontal functionalities that span across various aspects of an organisation's operations. These functions encompass key activities related to audits, monitoring, and security to safeguard the integrity, confidentiality, and availability of systems and data.

Figure 3 also shows interfaces which enable the communication between functions. Details of these interfaces are described as below.

a) Data acquisition interface

This interface, linked to the SCP, facilitates the collection of information from external sources. The features of this interface are described in 7.3.1.

b) Interoperability interface

This interface integrated with the SCP, allows for seamless communication with external data providers and third-party computational systems. The features of this interface are described in 7.3.2.

c) Service interface

This interface integrated with the SCP allows application-to-application access to utilise the support functions offered by the SCP as described in 7.3.3

7.3 Requirements for interoperability of Smart City Platforms (SCP)

To ensure an effective interoperability service, it is crucial to consider the following aspects.

a) Interoperability with different technologies

The capability to support various technologies for capturing information and communication standards, as well as integration with internal or corporate and external information systems.

b) Performance

The ability to efficiently handle a large volume of devices, services, and processes while maintaining optimal performance levels.

c) Scalability

The capacity to expand processing, interconnection, and storage capabilities without requiring significant architectural changes, allowing for seamless growth as the system evolves.

d) Robustness and resilience

The capability to continue functioning even in the face of problems, such as network failures or device malfunctions, by employing redundancy, fault tolerance, and appropriate error-handling mechanisms.

e) Security

The assurance of maintaining security and reliability throughout the interoperability service, safeguarding sensitive data, preventing unauthorised access, and ensuring secure communication and information exchange.

f) Extensibility

The adaptability of the interoperability service to accommodate new requirements and emerging technologies, enabling it to evolve and meet future needs without significant disruptions.

7.3.1 Acquisition interface

It is imperative that the acquisition interface of the SCP should adhere but not limited to the following technical characteristics:

a) Network access and sensor technology independence

This means compatibility with various network access methods and IoT or Machine-To-Machine (M2M) protocols, ensuring flexibility and adaptability.

b) Support for open protocols and protocol translation

This capability guarantees that the platform remains agnostic to device complexities, access to sensors and actuators from diverse manufacturers by facilitating the translation of different protocols.

c) Access to sensors or actuators

Information from sensors and actuators is gathered via a transport network, allowing for data collection.

d) Support for Security and Monitoring Functions

Robust security measures and continuous monitoring are embedded into the interface to safeguard data and operations.

e) Discovery and Access to IoT or M2M Applications

The interface provides the means to discover and access IoT or M2M applications, promoting versatility and application integration.

f) Support for device and application identification and naming

This feature ensures that devices and applications can be identified and named consistently within the platform, contributing to clarity and manageability.

7.3.2 Interoperability interface

It is essential that this interface facilitates interoperability between the SCP and external systems, allowing access to data, information, and services hosted or provided by the SCP.

Furthermore, the interface should incorporate authentication and authorisation components to manage access control to its functions. The permissions granted should align with the terms of use.

For optimal functionality, it is advisable that this interface supports internal access to the data management and core capabilities offered by the acquisition/interconnection functions, including the ability to perform the following activities.

a) Access metadata related to sensors registered in the platform.

b) Implement authentication and authorisation processes for various available actions.

c) Enable real-time data collection from individual sensors or groups of sensors.

It is advisable that this interface should adhere but not limited to the following.

a) Supports the manipulation of datasets by offering functionalities that enable mathematical operations on the data.

b) Facilitates extraction and analysis processes, providing capabilities for in-depth analysis of large datasets, thus transforming data into valuable and actionable insights.

c) Equipped to provide internal access to the information management services provided by the service support functions. This access can be achieved through the implementation of Application Programming Interfaces (APIs) that offer diverse data access modes, including push (subscription and notification) as well as pull (request and response) mechanisms.

7.3.3 Service interface

The service interface should meet but not limited to the following requirements.

a) It should offer a suite of APIs and supplementary tools, including a development kit and open data portals, which will be instrumental in implementing the services provided to clients.

b) It is imperative that the interface provides secure access to the APIs, development kit, web portal, and other associated tools.

c) The interface should be founded on open APIs, including the provision of an API manager, that can be leveraged by both internal and external applications. It should align with the prevailing standards and practices.

d) Offers a web portal that is accessible and usable in conjunction with the services it provides.

e) Supports diverse data access modes, encompassing both push (subscription and notification) and pull (request and response) methods, to cater to varying needs.

f) Provides the necessary mechanisms for adapting communications to accommodate different data models and semantics, ensuring compatibility and consistency.

Bibliography

[1] ISO/IEC 17788:2014, *Information technology — Cloud computing — Overview and vocabulary*

[2] ISO/IEC 21823-1. *Internet of Things (IoT) – Interoperability for IoT Systems – Part 1: Framework*

[3] ITU-T Y.4200, *Requirements for the interoperability of smart city platforms.*

[4] ITU-T Y.4201, *High-level requirements and reference framework for smart city platforms.*

[5] ETSI TR 103 536, v1.1.2, *SmartM2M; Strategic / technical approach on how to achieve interoperability / interworking of existing standardized IoT Platforms.*

Acknowledgements

Members of the Internet of Things (IoT) and Smart Sustainable Cities Working Group

Dr Gopinath Rao Sinniah (Chair/Draft Lead)	Favoriot Sdn Bhd
Mr Mohd Amin Mohd Din (Vice Chair)	Maxis Broadband Sdn Bhd
Associate Professor Dr Teng Kah Hou (Secretary)	UCSI Education Sdn Bhd
Mr Mohamad Norzamir Mat Taib (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Low Kien Yap/	CelcomDigi Berhad
Mr Ng Thian Boon	
Mr Ang Kah Heng/	Cyberview Sdn Bhd
Ms Athirah Tan Abdullah	
Ts Pang Jia Yew	Heriot-Watt University Malaysia
Mr Abbas Ali	Kiwitech Sdn. Bhd.
Mr Cheong Gze Wei/	Maxis Broadband Sdn Bhd
Mr Meng Keen Wai/	
Ms Norhanisah Mohd Basri	SIRIM Berhad
Professor Ts Dr Lau Sian Lun	Sunway University College Sdn Bhd
Mr Mohd Zakir Hussin Baharuddin	TM Technology Services Sdn Bhd
Dr Mohd Yamani Idna Idris	Universiti Malaya
Professor Dr Borhanuddin Mohd Ali	Universiti Putra Malaysia
Associate Professor Ir Dr Yusnani Mohd Yussoff	Universiti Teknologi MARA

By invitation

Mr Chin Wai Meng	Daikin Malaysia Sdn. Bhd.
Ms Nur Amilin Mohd Khazani	Jabatan Perancangan Bandar dan Desa
Ts Md Farabi Yussoff Md Yussoff	Jabatan Perancangan Bandar dan Desa
Dr Navaneethan Arjuman	NLTVC Education Sdn Bhd
Mr Mohamed Shajahan Mohamed Iqbal	Three-OPP (M) Sdn Bhd