TASMU Interoperability Policy

Document Information

Title: TASMU Interoperability Policy

Policy Reference: TASMU-INT-POL

Policy Number: 003/2020

Published Version: V1.0

Status of This Policy: FINAL DRAFT FOR PUBLICATION

Policy Abstract

The success of the smart nation depends on interoperability, achieved through using easily compatible technologies and following ecosystem rules. This is the TASMU Interoperability Policy which has been developed in order to get the most out of smart city suppliers, to remove the risk of silos and fragmentation, and to safeguard the sustainable evolution and expansion of the TASMU Ecosystem.

Copyright Notice

Requirements Language

The key words “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “NOT RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as follows:

- **SHALL**: This word, means that the definition is an absolute requirement of the policy.
- **SHALL NOT**: This phrase, means that the definition is an absolute prohibition of the policy.
- **SHOULD**: This word, or the adjective “RECOMMENDED”, mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT**: This phrase, or the phrase “NOT RECOMMENDED” mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- **MAY**: This word, or the adjective “OPTIONAL”, mean that an item is truly optional.

Normative References

[AMQP]

Advanced Message Queuing Protocol is an open standard application layer protocol for message-oriented middleware. The defining features of AMQP are message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security.

[Bluetooth]

Bluetooth is a wireless technology standard used for exchanging data between fixed and mobile devices over short distances using short-wavelength UHF radio waves in 2.400 to 2.485 GHz bands, for building personal area networks (PANs).

[Cellular]

A cellular network or mobile network is a communication network where the last link is wireless, served by the base stations, which provide the cell with the network coverage which can be used for transmission of voice, data, and other types of content. Currently, common mobile networks technology include 2G, 3G, 4G and 5G.

[CoAP]

Constrained Application Protocol (CoAP) is an application layer protocol that is intended for use in resource-constrained Internet devices, such as WSN nodes. CoAP is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized requirements such as multi-cast support, very low overhead, and simplicity.

[DDS]

Data-Distribution Service for Real-Time Systems, is an open international middleware standard directly addressing publish-subscribe communications for real-time and embedded systems.

[EC-GSM-IoT]

Extended Coverage-GSM-IoT enables new capabilities of existing cellular networks for LPWA (Low Power Wide Area) IoT applications. EC-GSM-IoT can be activated through new software deployed over a very large GSM footprint, adding even more coverage to serve IoT devices.

[Ethernet]

Ethernet is a family of computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN).

[gRPC]

gPRC gRPC is an open source remote procedure call (RPC) system. It uses HTTP/2 for transport, Protocol Buffers as the interface description language, and provides features such as authentication, bidirectional streaming and flow control, blocking or nonblocking bindings, and cancellation and timeouts. It generates cross-platform client and server bindings for many languages. Most common usage scenarios include connecting services in microservices style architecture and connect mobile devices, browser clients to backend services

[HTTP/2]

HTTP2 enables a more efficient use of network resources and a reduced perception of latency by introducing header field compression and allowing multiple concurrent exchanges on the same connection.

[HyperCat]

HyperCat is an open, lightweight JSON-based hypermedia catalogue format for exposing collections of URIs.

[IBM MessageSight]

IBM MessageSight is designed specifically for machine-to-machine (M2M) and Internet of Things scenarios, by supporting massive communities for concurrently connected end points.

[IEEE.802.15.4]

IEEE Standard for Low-Rate Wireless Networks is the protocol and compatible interconnection for data communication devices using low-data-rate, low-power, and low-complexity short-range radio frequency (RF) transmissions in a wireless personal area network (WPAN) are defined in this standard.

[Interoperability Framework]

ISBN 978-92-79-63756-8, New European Interoperability Framework, 2017, Publications Office of the European Union.

[ISA100.11a]

ISA100.11a is a wireless networking technology standard developed by the International Society of Automation (ISA). It is described as ‘Wireless Systems for Industrial Automation: Process Control and Related Application’.

[LLAP]

Lightweight Local Automation Protocol is a simple and short messaging protocol which can run on any communication medium. the protocol has been designed for direct messaging between embedded devices independent of the low level physical layer protocol used by the devices.

[LoRA]

LoRa is a low-power wide-area network (LPWAN) technology, is a proprietary, chirp spread spectrum (CSS) radio modulation technology for LPWAN used by LoRaWAN, Haystack Technologies, and Symphony Link.

[LoRaWAN]

The LoRaWAN specification is a Low Power, Wide Area (LPWA) networking protocol designed by LoRA Alliance, intended for wireless battery operated Things in regional, national or global network.

[LTE-MTC]

The LTE-Machine Type Communication, LTE-MTC is the simplified industry term for the LTE-MTC low power wide area (LPWA) technology standard published by 3GPP in the Release 13 specification.

[LWM2M]

LWM2M is a Lightweight M2M, LWM2M is a system standard in the Open Mobile Alliance. It includes DTLS, CoAP, Block, Observe, SenML and Resource Directory and weaves them into a device-server interface along with an Object structure.

[mDNS]

Multicast Domain Name System, Resolves host names to IP addresses within small networks that do not include a local name server.

[Mihini/M3DA]

The Mihini agent is a software component that acts as a mediator between an M2M server and the applications running on an embedded gateway. M3DA is a protocol optimized for the transport of binary M2M data.

[MiWi]

MiWi is a proprietary wireless protocol supporting peer-to-peer, star network connectivity. It was designed by Microchip Technology. MiWi uses small, low-power digital radios based on the IEEE 802.15.4 standard, and is designed for low-power, cost-constrained networks, such as industrial monitoring and control, home and building automation, remote control, wireless sensors, lighting control, and automated meter reading.

[Mosquitto]

Eclipse Mosquitto is an open source (EPL/EDL licensed) message broker that implements the MQTT protocol versions 5.0, 3.1.1 and 3.1. Mosquitto is lightweight and is suitable for use on all devices from low power single board computers to full servers.

[MQTT]

Stands for Message Queuing Telemetry Transport, MQTT is a machine-to-machine (M2M)/"Internet of Things" connectivity protocol. It was designed as an extremely lightweight publish/subscribe messaging transport. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium.

[MQTT-SN]

Stands for MQTT For Sensor Networks, MQTT-SN is an open and lightweight publish/subscribe protocol designed specifically for machine-to-machine and mobile applications.

[NB-IoT]

Stands for Narrow-Band IoT, NB-IoT is a low power wide area (LPWA) technology developed to enable a wide range of new IoT devices and services, the technology is standardized by the 3GPP standards body.

[NFC]

Stands for Near Field Communication, NFC is based on the standard ISO/IEC 18092:2004, using inductive coupled devices at a center frequency of 13.56 MHz. The data rate is up to 424 kbps and the rang with a few meters short compared to the wireless sensor networks.

[ONS 2.0]

Stands for Object Name Service, ONS uses the Internet's existing DNS for looking up (resolving) information about a GS1 Identification Key.

[OTrP]

Open Trust Protocol, a protocol to install, update, and delete applications and to manage security configuration in a Trusted Execution Environment (TEE).

[Physical Web]

The Physical Web enables visibility of a list of URLs being broadcast by objects in the surrounding environment with a Bluetooth Low Energy (BLE) beacon.

[Reactive Streams]

Reactive Streams is a standard for asynchronous stream processing with non-blocking back pressure on the JVM.

[REST]

Stands for Representational State Transfer and RESTful HTTP is a software architectural style that defines a set of constraints to be used for creating web services. Web services that conform to the REST architectural style, called RESTful Web services, provide interoperability between computer systems on the Internet.

[RPMA]

Stands for Random phase multiple access from Ingenu, RPMA is formerly known as On-Ramp Wireless. It is a proprietary technology, based on a variation of CDMA technology for cellular phones, but is purpose-built to use unlicensed 2.4GHz spectrum.

[SigFox]

SigFox is a network operator that builds proprietary wireless networks to connect low-power objects such as electricity meters and smartwatches, which need to be continuously on and emitting small amounts of data.

[SMCP]

SMCP is a C-based CoAP stack which is suitable for embedded environments. Features include: Support draft-ietf-core-coap-13, Fully asynchronous I/O, Supports both BSD sockets and UIP.

[SOAP]

Stands for Simple Object Access Protocol, SOAP is a messaging protocol specification for exchanging structured information in the implementation of web services in computer networks.

[IoT Interoperability]

ETSI SR 003 680 V1.1.1, TS SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach, 2020, ETSI.

[SSI]

Stands for Simple Sensor Interface, SSI is a simple communications protocol designed for data transfer between computers or user terminals and smart sensors.

[STOMP]

The Simple Text Oriented Messaging Protocol

[SynchroniCity]

SynchroniCity APIs, 2014, SyncroniCity.

[TASMU Security Policy]

TASMU Security Policy, 2020, TASMU

[UPnP]

Stands for Universal Plug and Play, UPnP managed by the Open Connectivity Foundation is a set of networking protocols that permits networked devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

[WebSocket]

The WebSocket specification developed as part of the HTML5 initiative introduced the WebSocket JavaScript interface, which defines a full duplex single socket connection over which messages can be sent between client and server. The WebSocket standard simplifies much of the complexity around bi-directional web communication and connection management.

[Weightless]

Weightless is a proposed proprietary open wireless technology standard for exchanging data between a base station and thousands of machines around it (using wavelength radio transmissions, although Weightless can operate in any frequency band, it is currently defined for operation in license-exempt sub-GHz frequency bands) with high levels of security.

[Wi-Fi]

Wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. Based on the IEEE 802.11 family of standards, Wi-Fi is a trademarked phrase for IEEE 802.11x.

[WirelessHART]

WirelessHART is a wireless sensor networking technology based on the Highway Addressable Remote Transducer Protocol (HART). The protocol utilizes a time synchronized, self-organizing, and self-healing mesh architecture, and supports operation in the 2.4 GHz ISM band using IEEE 802.15.4 standard radios.

[XMPP]

[Stands for Extensible Messaging and Presence Protocol, XMPP and is an open technology for real-time communication, which powers a wide range of applications including instant messaging, presence, multi-party chat, voice and video calls, collaboration, lightweight middle-ware, content syndication, and generalized routing of XML data.

[XMPP-IoT]

XMPP-IoT stands for XMPP for Internet Of Things.

[X.509]

X.509 is a ITU-T standard for public key infrastructure (PKI) to manage digital certificates and public-key encryption. A key part of the Transport Layer Security protocol used to secure web and email communication.

[ZigBee]

The ZigBee protocol uses the 802.15.4 standard and operates in the 2.4 GHz frequency range with 250 kbps. The maximum number of nodes in the network is 1024 with a range up to 200 meter. ZigBee can use 128 bit AES encryption.

Informative References

[SynchroniCity Architecture]

D1.3 Guidelines for SynchroniCity architecture, 2017, SynchroniCity

[SynchroniCity Reference Architecture]

D2.1 Reference Architecture for IoT Enabled Smart Cities, 2017, SynchroniCity

[SynchroniCity Reference Architecture Update]

D2.10, Reference Architecture for IoT Enabled Smart Cities, Update, 2018, SynchroniCity

[FIWARE Business API]

FIWARE Business API Ecosystem, FIWARE

[FIWARE NGSI]

FIWARE-NGSI v2 Specification, v2, FIWARE

[Internet of Things]

ITU-T, Y.2060 Overview of the Internet of things, 2012, ITU-T

[Internet of Things DEP]

ISO/IEC 30161, Internet of Things (IoT) - Requirements of IoT data exchange platform for various IoT services, 2019, ISO/IEC

[Semantic Interoperability]

ISO/IEC 21823-3 ED1, Internet of Things (IoT) - Interoperability for IoT Systems. Part 3: Semantic interoperability, 2019, ISO/IEC

[IoT Semantic Interoperability]

21st International Conference on Enterprise Information Systems: IoT Semantic Interoperability-A Systematic Mapping Study, 2019, Researchgate

[SmartM2M Semantic Interoperability]

ETSI TR 103 535 V1.1.1, SmartM2M; Guidelines for using semantic interoperability in the industry, 2019, ETSI

[SmartM2M Technical Interoperability]

ETSI TR 103 536 V1.1.2, SmartM2M; Strategic/technical approach on how to achieve interoperability/inter-working of existing standardized IoT Platform. 2019, ETSI.

[SmartM2M Ontology Mapping]

ETSI TS 103 264 V2.1.1, SmartM2M; Smart Appliances; Reference Ontology and oneM2M Mapping, 2017, ETSI

[SmartM2M Ontology]

ETSI TS 103 264 V3.1.1, SmartM2M; Smart Applications; Reference Ontology and oneM2M Mapping, 2020, ETSI

[Web of Things]

ITU-T Y.2063 Framework of the web of things, 2012, ITU-T

Contents

Definitions

The definitions used in this policy have been written to provide contextual clarity and where necessary specificity, and should not be interpreted to be contradictory to any laws in the State of Qatar.

[Acquisition Interface]

An acquisition interface refers to the TASMU System's data acquisition interfaces between the [TASMU Conceptual Diagram (G)/(H) and (F)], the Central Platform within the TASMU Ecosystem. They provide an interface to upper layers for easy data conversion without worrying about such complexity in lower layers.

[Autonomic Networking]

Autonomic Networking is the ability for a network and the nodes in that network for self-management, self-configuring, self-connecting, self-provisioning, self-healing, self-optimizing and self-protecting techniques and/or mechanisms.

[Building Blocks]

Refers to the smart city's building blocks, include infrastructure, enablers and digital solutions that support and operate TASMU Smart Service with underlying connectivities and infrastructure technologies.

[Common Technology]

Refers to the kind of smart city technologies which are commonly recognised, used and/or standardised by the credible international standard bodies, technology alliance, associations or proprietary technology organisations.

[Intercity Interfaces]

An intercity interface refers to the interface between the TASMU Central Platform and another smart city.

[Interplatform Interface]

The Interplatform Interface refers to the data exchange interfaces between the [TASMU Conceptual Diagram (J)] and [TASMU Conceptual Diagram (E) and (F)] within the TASMU Ecosystem.

[Internet of Things]

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, uniquely identified with the ability to transfer data over a network to Sector Platforms and/or the Central Platform.

[IoT Endpoint]

An IoT Endpoint is a physical computing device that performs a function or task as part of a TASMU Smart Service.

[Ontologies]

An ontology is a way of showing the properties of a subject area and how they are related, by defining a set of concepts and categories that represent the subject. It encompasses a representation, formal naming and definition of the categories, properties and relations between the concepts, data and entities that substantiate one, many or all domains of discourse.

[Open APIs]

An Open API is a publicly available application programming interface that provides developers with programmatic access to a proprietary software application or web service.

[Organisation Interoperability]

Refers to the way in which TASMU Service Operator aligns with the TASMU Smart Nation Regulator and other TASMU Systems processes, responsibilities and expectations to achieve commonly agreed and mutually beneficial goals.

[Semantic Interoperability]

Refers to the ability of two or more computational systems to exchange information through a shared meaning that can be interpreted automatically and unambiguously.

[Service Interface]

A service interface refers to the interfaces between smart application or service (C) and Sector data analytics platforms (E) within the TASMU Ecosystem.

[Subscriber]

An organisation or individual who utilises a TASMU Smart Service. They subscribe to and are authenticated by the TASMU Ecosystem. In some contexts they may be referred to as consumers.

[TASMU Common Policies]

These are a set of mutually exclusive baseline policies, that are best practice and required for any TASMU System operating within the TASMU Ecosystem.

[TASMU Ecosystem]

This is the Smart Qatar (TASMU) platform and any TASMU Smart Service that is either connected to this Central Platform or is branded as TASMU compliant. Refer to (A) in the TASMU Conceptual Diagram.

[TASMU Smart Nation Regulator]

The entity in the State of Qatar who regulates the TASMU Ecosystem. It is responsible for drafting, promoting, governing, updating, monitoring compliance with, and enforcing this policy.

[TASMU Smart Service]

A TASMU Smart Service is a national service, leveraging one or multiple technologies, to resolve an identified challenge or enable a desired outcome and that operates in the TASMU Ecosystem. Collectively, they focus on detailing and contextualizing services relevant for the State of Qatar.

[TASMU Service Operator]

This is the owner and operator of the TASMU System, who has overall responsibility for its secure, compliant operation.

[TASMU System]

This refers to any of the following elements from the TASMU Conceptual Diagram:

- (C) Any smart application or service
- (D) Any networking between platforms and (C)
- (E) Sector data analytics platforms
- (F) Central data analytics platform
- (G) Any networking between platforms and devices (H)
- (H) Any smart devices
- (I) The TASMU Control Centre
- (K) Security Management System of the TASMU Ecosystem
- (L) Operations Management System of the TASMU Ecosystem

[Technical Interoperability]

refers the ability of two or more technology applications within the ecosystem, to accept data from each other and perform a given task in an appropriate and satisfactory manner without the need for extra human intervention.

[Transport Network]

Refers to the public telecommunications infrastructure which permits telecommunications between and among defined network termination points.

[Uncommon Technology]

Uncommon technology refers to the kind of technology that is purposely developed, not recognised by the industry, not standardised and documented by the creditable international communities and standardisation bodies, nor developed with the open-source.

[Web of Things]

The Web of Things (WoT) is software architectural styles and programming patterns that allow real-world objects to be part of the World Wide Web. Similarly to what the Web (Application Layer) is to the Internet (Network Layer),the Web of

Things provides an Application Layer that simplifies the creation of Internet of Things applications composed of multiple devices across different platforms and application domains

1. Introduction

1.1 TASMU

The Qatar National Vision 2030 aims to “transform Qatar into an advanced society capable of achieving sustainable development.” TASMU, or the Smart Qatar program, is a digital response to the goals that have been set out in the National Vision 2030. It is about harnessing technology and innovation to improve quality of life and help drive economic diversification.

TASMU aims to leverage innovative applications of technologies to provide targeted services for residents, businesses and government across priority sectors. The foundation of this whole-of-nation effort relies on the ability to collect and manage vast amounts of data, share and open it up for spawning broad-based innovation and entrepreneurship within a set of defined rules and regulations. This is then processed and analysed by different actors for the build-up of innovative services and applications. As such, governance of TASMU on a national level has been designed to harmonize efforts across the different actors and drive Smart Qatar development with a key focus on ensuring efficiency and building resilience and interoperability.

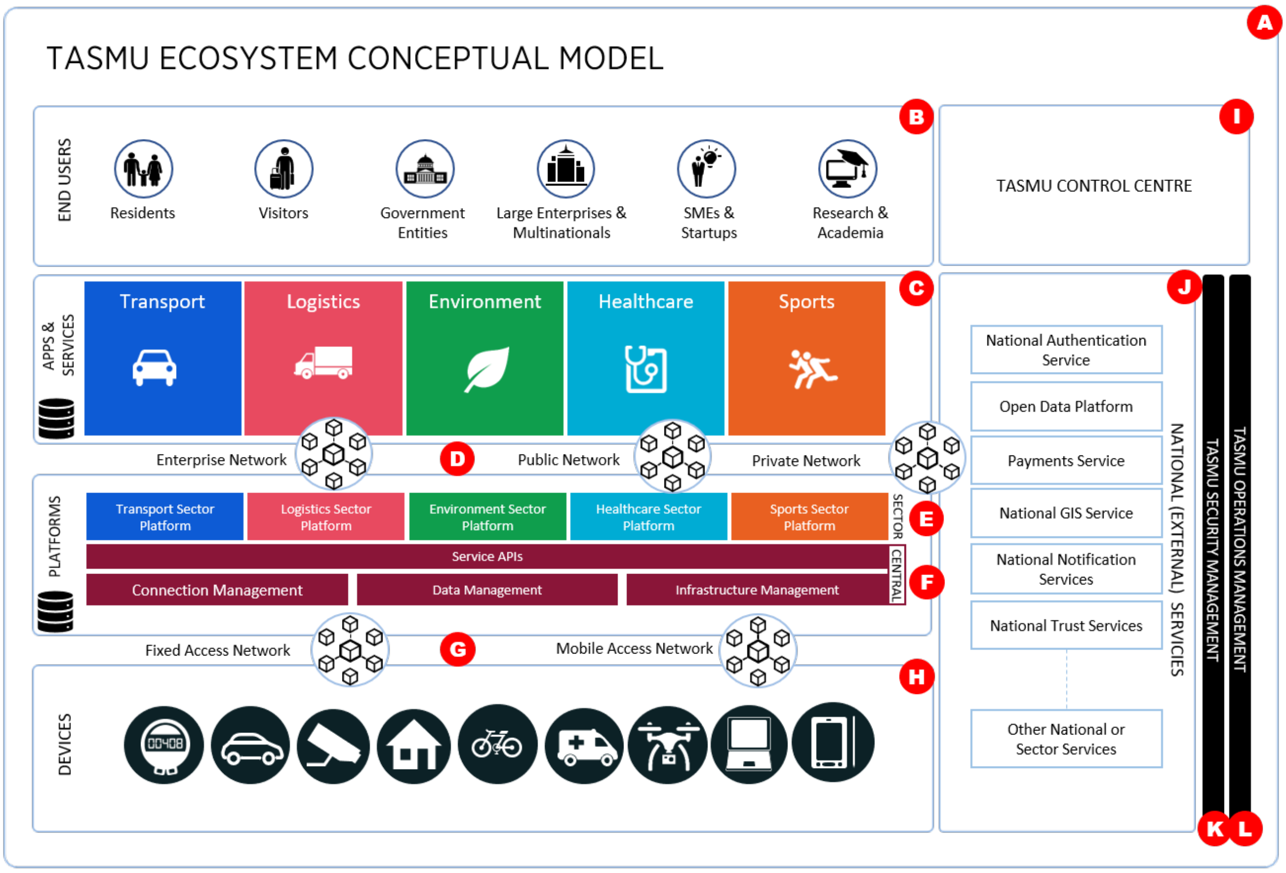
TASMU Smart Services are services designed to solve evolving challenges targeted constituents (people, businesses, or government) face, leveraging technology and innovation. TASMU Smart Services cut across industry sectors focusing on human, social, economic, and environmental development. They can be focused on providing convenience or entertainment, or could address critical needs such as national safety and security. As such, the type of information they leverage can range from publicly open to sensitive or private information.

1.2 TASMU Interoperability Policy

To ensure the efficiency and sustainable evolution of the TASMU Ecosystem, the TASMU Interoperability Policy provides overarching semantic and technical controls, as well as recommendations on organisational interoperability. Specifically it includes controls covering Internet of Things which have particular applicability.

This TASMU Interoperability Policy is regulated by the TASMU Smart Nation Regulator.

The policy covers the TASMU Ecosystem and interactions with it. The diagram below shows the TASMU Ecosystem in context to this policy.



Only the following elements are within the scope of this policy:

- C: is the TASMU Smart Services and services ecosystem
- D: are the network connections from the central platform, over enterprise, public and private networks
- E: are the sector data analytics platforms ('Sector Platforms')
- F: is the central TASMU data analytics platform ('Central Platform')
- G: is the Internet of Things (IoT) access network, either over fixed or wireless networks
- H: is the IoT devices ecosystem
- J: is the ecosystem of national services/platform that connects to the TASMU Central Platform and (C) above

1.3 Compliance

All TASMU Service Operators SHALL:

1. Comply with this policy where they operate a TASMU System or provide a TASMU Smart Service to a Subscriber, prior to operating in the TASMU Ecosystem and on a regular basis as directed by the TASMU Smart Nation Regulator.

2. Ensure that this policy is applied to all aspects of the TASMU System, whether that is maintained or operated by a third party, prior to operating in the TASMU Ecosystem.

3. Ensure this policy is considered in conjunction with the specific TASMU Smart Service sector policy issued by the TASMU Smart Nation Regulator or the sector regulator, which will cover specific requirements of the TASMU Smart Service.

4. Allow for an independent audit to check compliance, as and when necessary, or as directed by the TASMU Smart Nation Regulator.

5. Notify the TASMU Smart Nation Regulator, when the TASMU System undergoes, as applicable, any changes to the following:

   a. major changes in service applications, software or hardware components

b. changes in interoperability standards
c. changes in network technologies
d. changes in Common Technology
e. changes in the Central Platform or Sector Platforms, that affect the TASMU System
f. changes in Application Programming Interfaces (APIs) that affect the inter-working within TASMU Ecosystem

2. Interoperability Controls

2.1 Governance

The provisioning of a TASMU Smart Service often requires different public sectors to work together to meet end users' needs and provide both public and commercial services in an integrated way. When multiple sectors and organisations are involved there is a need for coordination and governance by the authorities with a mandate for planning, implementing and operating the services. Services should be governed to ensure integration, interoperability, seamless execution, and, reuse of services, data and Building Blocks. Hence, the following controls apply:

1. TASMU Service Operators SHALL develop Interoperability Agreements, or similar formal agreements, when their TASMU Smart Services integration covers more than one TASMU System or TASMU Ecosystem sector.

2. Where there is a requirement for an Interoperability Agreement it SHALL include at least:

   a. clear objectives and methods to achieve interoperability, while leaving each organisation the maximum feasible internal and national autonomy
   b. the governance structure for interoperability approach, management, approval and reviewing processes
   c. both general and sector standards and specifications at the semantic and technical levels
   d. a reasonable period of validity
   e. the limitations of interoperability
   f. the following aspects of interoperability:

      - quality
      - scalability
      - availability of reusable Building Blocks, including information sources (base registries, open data portals, etc.)
      - any other interconnected services

   g. the translation of external information/services into clear Service Level Agreements (SLA), covering interoperability
   h. change management provisions covering procedures and processes needed to deal with and control changes, ensuring the accuracy, reliability, continuity and evolution of the service
   i. business continuity/disaster recovery provisions to ensure that digital public services and their building blocks continue to work in a range of situations, e.g. cyber attacks or the failure of Building Blocks

3. Where there is a requirement for an Interoperability Agreement it MAY include:

   a. an agreed set of standards and specifications among the TASMU System
   b. other types of agreements among the TASMU System to complement, including:

      - memorandum of understanding (MoUs)
      - support/escalation agreements
      - technical documents for semantic and technical understanding

4. In the event of a disagreement about interoperability between the TASMU Systems parties, TASMU Service Operators SHALL present their cases to the TASMU Smart Nation Regulator for dispute resolution. TAMSU Service Operators SHALL make necessary changes or enhancements on the relevant TASMU Systems solution as necessary once they receive the decisions from the TASMU Smart Nation Regulator.

2.2 Solution Architecture

1. The architecture of the TASMU Smart Service SHALL clearly incorporate and show the following, as applicable:

    a. [TASMU Conceptual Diagram (H)]: IoT devices ecosystem, including device/data source layer and any smart devices
    b. [TASMU Conceptual Diagram (G)]: IoT access network
    c. [TASMU Conceptual Diagram (E), (F) & (J)]: data layer between these components
    d. [TASMU Conceptual Diagram (C)]: Application and services
    e. [TASMU Conceptual Diagram (L)]: Operations Management of the TASMU Ecosystem
    f. [TASMU Conceptual Diagram (K)]: Security and data protection, privacy layer

2. The TASMU Systems solution(s)SHALL provide capabilities to meet the following TASMU Smart Services criteria:

    - **performance:** ensure that there is no end-user service performance degradation, as the number of devices, services and load increases
    - **scalability:** ensure the processing, communications and storage can scale without requiring changes to the solution architecture
    - **robustness and resilience:** ensure the service rapidly and effectively protects its critical capabilities from disruption caused by adverse events and conditions
    - **security:** ensure compliance against the TASMU Security Policy
    - **extensibility:** ensure architecture and data-flows are unaffected or minimally affected by new or modified functionality

3. The TASMU Service Operator SHOULD use the capabilities of the Central Platform, Sector Platforms, IoT Access Network [[TASMU Conceptual Diagram (G)] and/or national services/platform [TASMU Conceptual Diagram (J)], as applicable, to form the core part of TASMU Smart Services.

4. The TASMU Service Operator SHALL obtain approval from the TASMU Smart Nation Regulator when their TASMU Smart Service uses capabilities from outside the TASMU Ecosystem.

2.3 Technical Interoperability

1. The TASMU Smart Service SHALL be interoperable with other TASMU Ecosystem technologies as follows, as applicable:

    a. [TASMU Conceptual Diagram (H)]: IoT devices ecosystem for capturing data
    b. [TASMU Conceptual Diagram (D), (G)]: network communications and IoT access network
    c. [TASMU Conceptual Diagram (E), (F)]: Sector Platforms and Central Platform
    d. [TASMU Conceptual Diagram (J)]: national services/platform, at a minimum, National Authentication, National Trust and Open Data

2. The TASMU Service Operators SHOULD use Open Development and Testing Services in [TASMU Conceptual Diagram (J)]: national services/platform for supporting developers in TASMU Smart Service development activities.

3. The TASMU Smart Service SHALL use Common Technology in order to reduce the complexity of interoperability.

4. The TASMU Smart Service SHALL NOT use Uncommon Technology without explicit approval from the TASMU Smart Nation Regulator.

5. The Acquisition Interface SHALL provide capability of collecting the sensor/actuators information through a Transport Network.

6. The Acquisition Interface SHALL be independent of network access and sensor technology.

7. The Acquisition Interface SHALL be compatible with at least one of the following network access technologies and/or IoT/M2M protocols:

    - Cellular

- Ethernet
- Bluetooth
- LoRA/LoRAWAN
- Weightless
- NB-IoT
- LTE-MTC
- EC-GSM-IoT
- RPMA
- gRPC
- IEEE 802.15.4
- WirelessHART
- MiWi
- ZigBee
- ISA100.11a
- SigFox
- Wi-Fi

8. The Acquisition Interface SHALL have a data interoperability approach to its design and support at least one of the following open protocols and/or protocol translators:

    - REST
    - MQTT
    - MQTT-SN
    - AMQP
    - CoAP
    - Websocket
    - SMCP
    - STOMP
    - XMPP
    - XMPP-IoT
    - Mosquitto
    - IBM MessageSight
    - Mihini/M3DA
    - DDS
    - LLAP
    - LWM2M
    - SSI
    - Reactive Streams
    - ONS 2.0
    - SOAP
    - HTTP/2

9. The Acquisition Interface SHALL support security and monitoring functions by using at least one of the following protocols:

    - OTrP
    - X.509

10. The Acquisition Interface SHALL provide functions for discovery and access to IoT application, and support at least one of the following protocols:

    - mDNS
    - Physical Web
    - HyperCat
    - UPnP

11. The Acquisition Interface SHALL provide functions for identification and naming of devices and applications.

12. The Interplatform Interface SHALL comply with the following requirements:

  a. enable interoperability between [TASMU Conceptual Diagram (J)] and the Sector Platforms and the Central Platform
  b. allow access to data, information and services that are stored or provided by [TASMU Conceptual Diagram (J)]
  c. include authentication and authorization control access to functions, which are determined by the third party platform’s terms of use
  d. comply with sector interoperability protocol requirements as applicable
  e. enable internal access to the data management and basic capabilities offered by the acquisition/interconnection functions:
     - to enable access to the meta data of sensors registered in the platform
     - to implement authorization and authentication functions for the different available actions
     - allow real-time collection of data generated by a sensor or group of sensors

13. The Interplatform Interface SHOULD include the following capabilities:

  a. provide functionalities that allow mathematical operations on the data
  b. allow extraction and analysis processing
  c. enable internal access to the information management offered by the service support functions through APIs
  d. enable APIs providing different data access modes, including push (subscription and notification) and pull (request and response)

14. The Service Interface SHALL provide the following common functionalities:

  a. authentication and authorisation
  b. accounting
  c. application data integration
  d. policy management
  e. performance evaluation
  f. event notification
  g. user interface

15. The Service Interface SHALL offer APIs, development kits and open data portals in order to implement the services for end users, and SHALL comply with the following requirements:

  a. provide a secure access to the APIs, development kit, web portal
  b. use standard and Open APIs that both the internal or external applications can use

16. The Service Interface SHOULD include:

  a. a web portal listing the services offered
  b. APIs providing different data access modes, including push (subscription and notification) and pull (request and response)
  c. the mechanism necessary to adapt the communications to the data models and semantics

17. The Intercity Interface SHOULD meet the SynchroniCity API requirements in order to ensure the State of Qatar can potentially share smart city data with other nations.

2.4 Semantic Interoperability

The interoperability at the semantic level requires a common understanding of the exchanged content’s meaning, preserving the semantics of the original message. To ensure the interoperability of applications and platforms in the TASMU Ecosystem, the semantic interoperability approach needs to create a common vocabularies which are capable of describing the meaning of a large amount of data that is in various formats and generated by different smart devices.

The TASMU Service Operator SHOULD follow the TASMU Smart Nation Regulator and sectors' guidance, and adopt the following good practices in development, design and implementation in order to achieve Semantic Interoperability within the TASMU Ecosystem:

1. Anticipate and include Semantic Interoperability and Ontologies at the early stage design and development of a TASMU Smart Service, in order to ease the cost and integration burdens of mass scale device deployment and avoid vendor lock-in.

2. Use one of the following approaches to achieve Semantic Interoperability:

   a. by standardisation, where platforms agree on whole or part of a common standardised model; or
   b. by mapping, where some translation "logic" is applied between different models.

3. Define a knowledge perimeter of the Ontologies to be used, including the set of concepts and relationships that are used in a Semantic Interoperability specification. This SHOULD:

   a. create suitable size of knowledge perimeter, ensure the effectiveness and completeness of the semantic specification.
   b. when using cross sector Ontologies, avoid accessing an entire sector specific Ontology. Instead, create the subset that is useful to build a cross sector Ontology.

4. Adopt both co-creation and separation-of-concerns design principles:

   a. use separation-of-concerns between sector experts and Semantic Interoperability experts, in which the former focuses on functional interoperability specification while the latter focuses on Ontology creation expertise
   b. use co-creation between the sector engineering, Semantic Interoperability experts and possible other categories of experts such as security and privacy experts, or user-centric design experts

5. Use a modular approach when designing Ontologies that focuses on the structuring of a wider concept into multiple and simpler sub-concepts that can be handled separately. In terms of Ontologies, sub-concepts are described by sub-Ontologies, which:

   a. use self-contained knowledge
   b. can be designed, used and maintained stand-alone
   c. are loosely coupled among themselves through well-defined relationships thereby enabling the preservation of the semantic richness of the wider Ontologies
   d. are consequently reusable.

6. Evaluate the maturity of Ontologies in two dimensions:

   a. Ontologies readiness, which measures maturity of the knowledge specification
   b. specification readiness, which measures the maturity of the interoperability specification

7. Use and maintain the following Ontologies:

   a. service discovery as an interoperability mechanism to discover a profile
   b. provision profile that supports specific optional features
   c. evolution or enhancement consideration in the Semantic interoperability specifications for matching the needs of different generations of products
   d. define rules for version management, such as upwards or backwards compatibility

2.5 Organisational Interoperability

In practice, organisational interoperability means documenting and integrating or aligning business processes and relevant information exchanged. Organisational interoperability also aims to meet the requirements of the user community by making services available, easily identifiable, accessible and user-focused. As many TASMU Smart Services are designed for large scale, cover multiple sectors and may cover deployment by many organisations, the TASMU Service Operator SHOULD adopt the following organisational interoperability good practices:

1. Ensure holistic governance of interoperability activities across administrative levels and sectors.

2. Use a structured, transparent, objective and common approach to assessing and selecting standards and specifications. Take into account relevant recommendations and seek to make the approach consistent across sectors. Check compliance and test their interoperability.
3. Document both internal and cross sectors interoperability related business processes using commonly accepted modelling techniques.
4. Clarify and formalise the organisational relationships between co-dependent TASMU Service Operators.

2.6 Internet of Things

The Internet of Things is one of the key components in many TASMU Smart Services. In order to ensure the interoperability between the Internet of Things and upper technology layers TASMU Service Operators SHALL ensure that any TASMU Smart Services with IoT Endpoints comply with the following requirements:

1. **Support identification-based connectivity:** See TASMU Security Policy on IoT Endpoint identification requirements.
2. **Support interoperability:** interoperability needs to be ensured among heterogeneous and distributed systems for provision and consumption of a variety of information and services.
3. **Support autonomic networking:** use Autonomic Networking in the provisioning and control functions of the IoT Endpoint in order to adapt to different application domains, different communication environments, and a large number of devices of various types. Autonomic services MAY depend on the techniques of automatic data fusion and data mining.
4. **Provide location-based capabilities:** where applicable, location-based capabilities need to be supported in the IoT Endpoint for some TASMU Smart Services functions that depend on the location information of things and/or users, in order to sense and track the location information automatically.
5. **Enable plug and play:** Plug and play capability needs to be supported in the IoT Endpoint in order to enable on-the-fly generation, composition or the acquisition of semantic-based configurations for seamless integration and cooperation of interconnected things with applications, and responsiveness to application requirements.
6. **Ensure manageability:** Manageability needs to be supported in the IoT Endpoint in order to ensure normal network operations. IoT applications usually work automatically without the participation of people, but their whole operation process should be manageable by the relevant parties.
7. Ensure the IoT Endpoints comply with the following requirements:
   a. they provide high quality and highly secure services for capturing, communicating and processing the data related to sector static features and dynamic behaviour with or without human intervention
   b. comply with the relevant sector’s laws, policies and standards, as defined in the applicable TASMU Smart Service policy.