Communications Regulatory Authority
State of Qatar

هيئة تنظيم الاتصالات
دولة قطر

Position Paper on IoT and M2M in Qatar

TABLE OF CONTENTS

Terms and Definitions

AI	Artificial Intelligence
BLE	Bluetooth Low Energy
CRA	Communications Regulatory Authority of Qatar
CSP	Connectivity Service Provider
eSIM	Embedded SIM. A chip that is hard-wired into as mobile device that can have SIM profiles downloaded to it.
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity. A technical number used by mobile networks to identify a user.
IoT	Internet of Things. A network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves.
IoT Device	A component in IoT that are programmed for certain applications, and which can transmit data over the internet or other networks
IoT End User	A person or organization that interacts with an IoT device.
IoT Sensor	A component in IoT that collects data from the environment.
IoT Service Provider	An organization that provides services that are used by IoT devices.
IoT-M	IoT - Machine. A service offered by mobile networks which is optimized for machine-to-machine communications.
ITU	International Telecommunication Union, the United Nations specialized agency for digital technology
IP	Internet Protocol
IPv6	The latest addressing scheme for internet connected devices.
LoRa	Long Range. A low power radio link protocol
LoRaWAN	LoRA Wide Area Network.
LTE	Long Term Evolution. Otherwise known as 4G.
M2M	Machine to Machine Communications.
MAC Address	A unique physical address specific to an Ethernet network.
MQTT	Message Queuing Transport and Telemetry. A protocol for transmitting messages between devices without reliable connectivity.
MSISDN	Mobile Subscriber ISDN Number. A number that mobile networks use identify a subscriber.

NB-IoT	Narrow Band IoT. A service offered by mobile networks, which provides low power communications but with low data rates.
NCSA	National Cyber Security Agency
NDPO	National Data Privacy Office
P-GW	Provider Gateway, a device in a mobile network that connects mobile user to external networks, including the internet.
Service Provider	An organization, typically a mobile network operator, that offers commercial telecommunications services.
SIM	A module that is inserted into a mobile device providing an identify for mobile network.
Telecommunications Equipment	Physical hardware that plays a role in delivering telecommunications services.
Type Approval	A certificate of conformity that is granted for a device make and model which authorizes its use in a particular country.

1 Context and Objectives

1.1. Executive Summary

The rapid pace of innovation in the ICT sector means that markets players often face the challenge of introducing new products and services into the market without a well-defined regulatory framework. An example of such recent emerging technology developments are Internet of Things (IoT) and Machine to Machine (M2M), which are broadly referred to as networks of devices that exchange data with other devices. These technologies are being implemented currently globally to build digital solutions and services and are also considered to have significant commercial implications for the telecom service providers and the rest of the IT industry in Qatar. Broadly, government, enterprises and consumers will stand to benefit from the opportunities that IoT/M2M technologies can provide in terms of operating efficiencies and new data related services. With an increased uptake, IoT/M2M does raise a number of regulatory issues (for example, spectrum, numbering, data security), with currently no specific regulatory framework for it in Qatar. This creates uncertainty and risks for service providers and end users in terms of safety and security, commercial viability and technical implementation.

One of the current strategic initiatives of Communications Regulatory Authority (CRA) aims at developing an IoT/M2M regulatory framework. This paper sets out on a high level the key elements and areas for CRA as considered for this framework.

Similarly, the Third Qatar National Development Strategy (NDS3)[1] emphasizes development of Qatar's digital economy and long-term strategic capabilities in emerging technologies to drive its growth.

CRA aims to develop IoT regulations aligned with the strategic priorities and targets set by QNV2030, NDS3 and Digital Agenda 2030 that focus around creating an environment for innovation, attracting investments, and positioning Qatar as an open for business regional and global digital hub and a leader in innovation and adoption of emerging technologies, accelerating progress towards a diversified, knowledge-based economy and sustainable development by 2030.

The global IoT ecosystem is transformative, providing significant benefits such as

[1] https://www.psa.gov.qa/en/nds1/nds3/Documents/QNDS3_EN.pdf

improved efficiency, cost savings, enhanced data insights, and the ability to create new business models and services. It is a key instrument to attract foreign investment, promote local entrepreneurship, and to generate employment opportunities, which aligns with Qatar's vision for a dynamic and diversified economy. However, IoT as an emerging technology also poses challenges, including the need for robust security, data privacy, and regulatory compliance.

Therefore, it is the aim of the CRA to establish a framework that fosters innovation and digital growth while compelling providers to act responsibly and not place consumers or the state at risk. Effective regulation shall ensure IoT deployments prioritize user privacy, data security, and interoperability, building stakeholder trust and encouraging adoption. The aim of the CRA is to be as light touch as possible.

The CRA is publishing this position paper detailing the potential regulatory approach so that stakeholders may benefit from it.

1.2. Document Scope and Approach

This document outlines the CRA's regulatory positioning on IoT/M2M with the goal to provide guidance to Internet of Things (IoT) ecosystem – government stakeholders, investors, entrepreneurs, service providers and IoT providers, and to promote safe, secure, and efficient adoption of IoT technologies and support Qatar's economy digitalization and diversification. The CRA regulatory position aims to support the national development goals and ensure compliance with international standards. The document provides an overview of the IoT and M2M as emerging technologies and summarizes use cases before going into some detail about those considered most relevant for the Qatar context. It concludes with a section on how CRA sees further the IoT regulatory framework to be implemented along with details on the technical standards to be adhered to within the annexure.

We shall note that regulatory aspects seen relevant to IoT ecosystem need to be addressed by at least several governmental authorities in Qatar. For example, regulations for IoT security aspects fall within the domain of the National Cyber Security Agency. This document does not aim to detail regulatory approaches that fall within the mandate of other authorities; however, the main regulatory aspects have been reviewed in a holistic manner on a high level.

In order to derive a comprehensive set of regulatory focus areas (Section 3), a framework of the ecosystem has been developed using a value chain approach as shown in

annexure II. We have also performed a global trends benchmark and considered the ones relevant to Qatar. A key input to the process is the strategic vision laid out in QNV2030 and the NDS3. Although IoT is not explicitly mentioned in QNV2030 or NDS3, emerging technologies in general are stated as pivotal for Qatar's economic diversification, growth and sustainability.

Earlier in 2023, the CRA has conducted an extensive study, 'Developing a Governance Framework for the Digital Economy in Qatar', which identified the key stakeholders and established the strategic importance of IoT, among other emerging technologies, as relevant to Qatar. This study concluded that there are no government bodies currently that specifically license or have an authorization regime for IoT services and applications, apart from the general business registration process that needs to be followed by companies.

This Position Paper has been developed considering comprehensive inputs from 30+ key industry stakeholders consulted, including ministries (Ministry of Communications and Information Technology (including TASMU), Ministry of Commerce and Industry, etc.) and other industry stakeholders (telecom service providers, businesses, Qatar Investment Authority, etc.). A concise summary of the insights built is presented in Section 2.3.

1.3. Definition of IoT and M2M

The terms Internet of Things (IoT) and Machine-to-Machine (M2M) are often used interchangeably, but they refer to slightly different concepts within the broader landscape of connected devices. Both IoT and M2M involve the communication between devices, but the scope and functionality of each are distinct.

For the purposes of this position paper, the following definitions have been adopted:

Internet of Things (IoT):

IoT refers to a network of interconnected physical devices embedded with sensors, software, and other technologies that enable them to collect and exchange data over the internet. These devices, ranging from household appliances to industrial machinery, can communicate with each other and with central systems, allowing for the automation of processes, real-time monitoring, and enhanced decision-making. IoT facilitates seamless integration between the digital and physical worlds, creating opportunities for improved efficiency, innovation, and user experiences across various sectors.

Machine-to-Machine (M2M):

Machine-to-Machine (M2M) communication is a subset of IoT that focuses specifically on the direct exchange of data between devices without human intervention. M2M technology enables devices to connect and communicate over wired or wireless networks, allowing them to perform tasks such as monitoring, control, and automation. This technology is commonly used in applications like remote monitoring, smart meters, and industrial automation, where devices need to transmit data to central systems or other machines for analysis and action.

IoT and M2M both involve the communication between devices, enabling the monitoring, control, and automation of various processes, often without human involvement. However, while M2M is primarily concerned with direct, point-to-point communication between specific machines, often within closed networks, IoT encompasses a broader and more complex network of devices that communicate over the internet.

M2M typically involves one-to-one or one-to-few relationships, using appropriate modes of wireless or wired connections for specific industrial or business applications. In contrast, IoT creates an interconnected ecosystem where data from various sources is aggregated, analyzed, and utilized across multiple platforms and applications, enabling interactions not just between machines but also between machines and humans.

In essence, M2M is a foundational technology within the broader IoT landscape. While M2M focuses on direct device-to-device communication, IoT expands this concept by integrating devices into a larger digital ecosystem, offering more extensive functionality, scalability, and integration possibilities.

1.4. Strategic Importance of IoT Regulation

The CRA recognizes IoT's strategic role in driving economic growth, improving quality of life, and fostering innovation. Establishing a clear IoT position will accelerate adoption, unlock its potential, and position Qatar as a leader in emerging technologies.

Economic Growth

IoT drives economic progress by optimizing operations through real-time data, reducing costs via automation and predictive maintenance, and enabling new business models like remote monitoring and subscription-based services. It also creates jobs in technology, AI, and system integration while fostering entrepreneurship.

Enhancing Quality of Life

IoT transforms daily life with smart cities offering efficient traffic management, energy use, and public safety. In healthcare, IoT enables remote monitoring and personalized medicine, while environmental sustainability benefits from smart meters, agriculture, and efficient transportation reducing resource use and emissions.

Fostering Innovation

IoT facilitates cross-sector collaboration, continuous improvement via real-time data analysis, and serves as a foundation for AI, machine learning, and blockchain, driving further advancements across industries.

1.5. Legal Basis

This paper has been created by the CRA that derives its powers from Decree No. (34) of 2006 and its amendments No. (17) of 2017 issuing the Telecommunications Law (the "Telecom Law"); where:

- Article 2(1) of Telecommunication law promulgated by Decree-Law No. (34) of 2006, as amended mandates that the CRA achieves the objective of "developing the Telecommunications sector in order to promote national, social and economic development".

- Article 2(2) of Telecommunication law promulgated by Decree-Law No. (34) of 2006, as amended mandates that the CRA must perform its duties and exercise its authority to, "improve the performance of the Telecommunications sector in the State, by encouraging competition and promoting reliance on Telecommunications services".

- Article 2(4) of Telecommunication law promulgated by Decree-Law No. (34) of 2006, as amended mandates that the CRA must carry out its duties and exercise its authority to, "increase benefits to customers and protect their interests".

- Article 4(1) of Telecommunication law promulgated by Decree-Law No. (34) of 2006, as amended mandates that the CRA must carry out its duties and exercise its authority to, "grant, modify, renew, suspend and revoke Class Licenses and Permits and Licenses to use The Frequency Spectrum, and determine the conditions and procedures for their issuance".

- Article 4(3) of Telecommunication Law promulgated by Decree-Law No. (34) of 2006, as amended mandates that the CRA must carry out its duties and exercise its authority to, “develop and manage the Frequency Spectrum plan and other scarce resources ensuring optimal use and maximizing their revenues to the extent required by International Rules”.

- Article 4(7) of Telecommunication Law promulgated by Decree-Law No. (34) of 2006, as amended mandates that the CRA must perform its duties and exercise its authority to, “draw up and manage the National Numbering Plan, and allocate numbers to Service Providers.

- Article 4(11) of Telecommunication law promulgated by Decree-Law No. (34) of 2006, as amended mandates that the CRA must perform its duties and exercise its authority to verify “compliance with the provisions of this Law and its implementing regulations, and the rules and decisions issued in the implementation procedure. The Secretariat-General, in order to achieve this, may use the services of specialized agencies, and academic or technical institutions or qualified consultants, to help perform some tasks and functions and cooperate and coordinate with ministries and other government agencies, bodies and public institutions.

Furthermore, the following laws have also been considered as listed below:

- Law No. (13) of 2016 on Privacy and Protection of Personal Data.

- Law No. (8) of 2018 on Consumer Protection.

- Law No. (16) of 2010 on Electronic Commerce and Transactions.

Additionally, the following references are relevant to the issues discussed in this document. Resolution of the Board of Directors of the Supreme Council for Communications and Information Technology No. (1) of 2009 issuing the executive regulations of the Telecommunications Law:

- Article (24) Clause (3) stating “Ensure that the use of radio spectrum is consistent with the national frequency assignment plan, related allocations and assignments, any applicable international treaties, commitments, protocols and standards and Radio Spectrum License conditions, including taking related compliance and enforcement actions.”.

- Article (24) Clause (5) stating “Determine, allocate, and assign, and re-allocate or re-assign, radio frequencies and frequency bands and channel assignments, and issue Radio Spectrum Licenses or radio frequency Authorizations, in accordance with the national frequency assignment plan”.

- Article (24) Clause (10) stating “Issue regulations, rules, orders or notices relating to the use of radio spectrum as the General Secretariat deems appropriate”.

- Article (24) Clause (11) stating “Determine any other matters relating to the transmission of radio-communications whether by satellite, terrestrial or other transmissions”.

The Communications Regulatory Authority (CRA) is the communications regulator of the State of Qatar established by virtue of the Emiri Decision 42 in 2014.

- Article (4) Clause (7) stating “Managing scarce resources, such as radio spectrum, numbers and domain names, and ensuring optimal use thereof”.

- Article (4) Clause (10) stating “Specifying standard criteria for the quality of performance of various services and monitoring compliance with these criteria by the authorities licensed to provide such services”.

- Article (4) Clause (11) stating “Establishing the standards and procedures that are necessary for the accreditation of telecommunication devices and equipment, including the devices and equipment that have been already accredited from other countries, and issuing licenses and approvals related thereto”.

- Article (4) Clause (15) stating “Any other duties or competences vested in it under the legislations in force”.

2 Current State of IoT in Qatar

2.1. Qatar’s Digital Vision

Qatar's modernization plans aim to balance economic growth with cultural preservation, guided by the Qatar National Vision 2030 (QNV2030) and its four pillars: human, social, economic, and environmental development. The Third National Development Strategy (NDS3) builds on QNV2030, targeting 4% non-hydrocarbon growth annually until 2030, with IT, digital technologies, and AI prioritized for economic diversification.

NDS3 emphasizes private-sector adoption of emerging technologies, establishment of national programs for digital transformation, cloud commercialization, and a cybersecurity framework. The Digital Agenda 2023 (DA2023) outlines strategies to adopt key technologies like AI, IoT, blockchain, and the metaverse.

The CRA focuses on advancing IoT adoption through regulatory improvements, addressing supply chain challenges, and fostering research collaborations to build a robust IoT ecosystem. These efforts aim to enhance operational efficiency, attract investment, and generate employment while positioning Qatar as a regional IoT leader.

By aligning IoT regulations with national priorities, Qatar seeks to ensure data security, privacy, and accessibility, fostering stakeholder trust and accelerating innovation. This approach supports the vision of a diversified, knowledge-based economy, driving sustainable development and improving quality of life by 2030.

2.2. Qatar's IoT Landscape Insights

The CRA has assessed the Qatari ecosystem and spoken to various stakeholders across key public and private sector entities, including service providers, public authorities, commercial organizations, educational and financial institutions, to understand their readiness and current state of IoT adoption across the country and noted that:

- **Proactive IoT Planning:** Many Qatari organizations have clear strategies and implementation roadmaps, showing promising progress in IoT adoption.
- **Early Benefits Realized:** Most entities have integrated IoT use cases like asset tracking, traffic monitoring, and health and safety, with advanced applications such as smart meters gaining traction.
- **Pragmatic Implementation:** While on-premises solutions are common, organizations increasingly leverage public, private, and hybrid clouds to meet diverse needs.

In addition to the primary inputs received by key stakeholders, the CRA also conducted a benchmarking study to understand the adoption of IoT services globally and upcoming trends in this domain, and noted that:

- IoT adoption is growing globally, with regulators developing guidelines, but connectivity and numbering challenges persist.

- Data portability issues risk vendor lock-in, and cross-border data flow remains complex.
- SIM usage ambiguities and regulatory hurdles hinder adoption for non-telecom providers.
- Interoperability, uncertified devices, and liability complexities challenge IoT deployment, despite emerging protocols like HTTPS and MQTT.
- IoT solutions rely on 5G for advancement, but critical infrastructure demands stricter standards.
- Privacy, security, and resilience concerns impact critical IoT systems and consumer confidence.
- Lack of dedicated IoT consumer laws and skilled workforce limits adoption and innovation.

2.3. Qatar's IoT Landscape Issues and Challenges

The adoption of IoT in Qatar encounters certain challenges, including limitations on the total number of connections (e.g., the 5-SIM cap) for expatriates and the absence of clear regulations specific to IoT. Issues related to device interoperability, compounded by the lack of standards for uncertified devices, impede seamless communication and accountability. Additionally, insufficient guidance on permanent roaming affects international IoT connectivity. Stakeholders have highlighted the necessity for collaborative frameworks and tailored guidelines to address interoperability, service quality, and security concerns across various sectors.

The complexity of IoT environments and governance, coupled with high costs and limited budgets, adds to the difficulty of scaling IoT solutions. The shortage of skilled professionals, combined with low user awareness about IoT risks and opportunities, further slows adoption. Regulatory gaps around licensing, spectrum allocation, data portability, and consumer protection exacerbate these challenges, making it crucial for CRA to establish clear standards, foster collaboration, and support capacity-building initiatives to drive IoT growth in Qatar.

Finally, data privacy, security, and resilience in critical IoT systems remain significant concerns, requiring robust measures to safeguard sensitive information and ensure service reliability. Addressing these issues, alongside consumer protection and liability in IoT ecosystems, will be pivotal for fostering trust and accelerating sustainable IoT

adoption across the country.

The details of each area identified as an issue or challenge have been detailed out within annexure III of this document along with CRA's recommendations for each area.

3 Regulatory Focus Areas

3.1. Introduction to Key Focus Areas

The CRA has assessed the feedback from stakeholders and highlighted areas requiring regulatory focus relevant to the adoption of IoT in the State of Qatar. This section sets out the current views of the CRA and how these should be addressed in terms of regulation and best practice.

Approach for each focus area has been developed based on the industry research undertaken by CRA and aligned with the CRA's mandate. The objective, as far as possible, should be that where regulation is required, it should be relatively light touch.

Following this consultation, the CRA will develop a framework document setting out the specifics relating to IoT policy and regulations.

3.2. Network and Equipment

Separation of Connectivity and Equipment

The CRA believes that customers should have the flexibility to purchase connectivity independently of equipment for IoT and M2M services. This approach promotes consumer choice and fosters a competitive market environment, ensuring customers can select the most suitable and cost-effective connectivity solutions for their needs. By separating connectivity from equipment, the CRA encourages innovation and competition among service providers, ultimately benefiting consumers with better service quality and pricing.

This policy aligns with Qatar's vision to support the growth of emerging technologies and creates a dynamic and adaptable telecommunications ecosystem that meets the evolving demands of IoT and M2M applications.

Device Certification

The CRA's position is that all IoT and M2M service devices sold or used in Qatar must undergo a dedicated approval process by the CRA. Ensuring that the devices meet

established certification standards is crucial for maintaining the telecommunications network's integrity, security, and reliability. Uncertified devices pose significant risks, including potential interference with network operations, security vulnerabilities, and compromised service quality. By enforcing stringent certification requirements, the CRA shall aim to protect consumers, promote a secure and robust IoT and M2M ecosystem, and support the sustainable growth of emerging technologies in Qatar. Type Approval process of CRA is expanded below.

Customer Advice

The CRA will publish periodic advice to users of IoT devices, highlighting the requirements for approval, as well as other advice which will help customers to understand their responsibilities.

The CRA advises customers to ensure that any devices they use for IoT and M2M services in Qatar are properly approved for use. Using uncertified devices can lead to significant risks, including network interference, security vulnerabilities, and compromised service quality. Customers should verify that their devices meet the established certification standards to protect themselves and ensure optimal performance. This measure is essential for maintaining Qatar's telecommunications network's integrity, security, and reliability.

3.3. Type Approval

All IoT devices sold in the State of Qatar will require Type Approval based on their perspective use and/or their connectivity with the existing communication networks for provisioning of IoT services. This is to prevent poor quality devices causing interference to other users or compromising the integrity of communication networks. The CRA has established a process for Type Approval which is available on CRA’s website. It is the responsibility of the equipment manufacturers, supplier of devices or the users to obtain such Type approval.

An exception exists whereby a device is legally registered on a mobile network outside of Qatar and is brought to Qatar and then connects to a Qatari mobile network (in-bound roaming). In this case, provided the device has type approval in the home country, then it may be permitted, subject to the permanent roaming conditions defined in this document. If, however, a service provider determines the device to be causing interference to other users, it may block the IMEI of the device. No such exception exists for devices that operate in unlicensed frequency bands.

Applicants will be required to pay a processing fee and provide appropriate technical data in accordance with the requirements specified by the CRA for type approval. Under certain circumstances, the applicant may also be required to make a physical device available for testing.

In the event that the CRA rejects the application for Type Approval, an appeal process will be provided, and an option for re-application will exist where manufactures are able to resolve underlying issues.

3.4. Connectivity Market Provision

The success of IoT depends upon innovation and competition among licensed connectivity suppliers and the CRA believes that there is a role that might be served by dedicated IoT wholesale connectivity providers. Such companies would likely resell services provided by the current service providers and purchase IoT connectivity on a wholesale basis for supply to IoT customers.

In most of the use cases shown in annexure II, for example urban management for smart cities, connectivity must be high speed, reliable and low latency. The cost of data should not prohibit the commercial viability of developing user applications. Service providers may therefore be required to offer network capacity to 3rd party service providers on the same basis as their own direct customers with no restrictions.

The CRA prefers that such companies enter into mutually beneficial commercial relationships with existing service providers but is prepared to intervene if this cannot be achieved without new regulation.

Following a review into CSP best practices, the CRA envisages service providers making available LTE, 5G, NB-IoT and LTE-M services, along with the necessary network interconnectivity, policy control, provisioning and billing APIs, access to SIM / eSIM profiles, and relevant support services. Low latency services are considered important for some real-time IoT use cases.

IoT providers that offer services that are business critical or those that have high availability requirements, including safety critical applications, may decide to deploy devices with multiple redundant network connections. The obligation and associated liabilities for determining whether the service levels offered by service providers are sufficient for the application rests with the designer of the application.

3.5. Identifiers

Number Allocation

The CRA's position to maintain the current number block allocation scheme, where MSISDNs are assigned to licensed operators in blocks of 100,000 and/or 10,000 numbers, offers significant benefits. This approach streamlines management, minimizes fragmentation, and enhances operational efficiency, facilitating smoother coordination and resource allocation for service providers. It also supports the sustainable growth of the telecommunications sector while ensuring effective use of available number resources. Furthermore, operators are only required to pay annual maintenance charges for the numbers, reducing financial burdens and enabling more predictable cost planning.

Number Range – Long MSISDNs

The CRA believes that the current MSISDN length is well-suited to the existing IoT/M2M market in Qatar, offering a practical and efficient solution to meet the telecommunications infrastructure's current and near-term requirements without causing unnecessary disruption. However, the CRA remains open to reassessing this approach in response to the growth of the IoT/M2M market in the country. Should the need arise, the CRA may consider extending the MSISDN length, such as adopting 12-character MSISDNs for IoT/M2M numbers.

Number Portability

Number portability exists to allow customers the ability to change service provider without the inconvenience of losing their phone number. Although some IoT use cases depend upon the devicehaving an MSISDN, the specific number used is less relevant. MSISDNs in IoT are mainly used forSMS communication, and since M2M is device to device, the numbers used are necessarily used by other devices, which can be reprogrammed to use new numbers.

The most common use cases for IoT exclusively involve packet data sessions and MSISDNs are not used. The CRA, therefore, does not regard number portability to be a major concern for IoT services. CRA recommends that the current IoT numbering range allocated to Qatari service providers shall be used for IoT service provisioning and number portability shall not be allowed for IoT numbers.

International Numbers and Roaming

The ITU makes available +88 country codes for international services. In agreement with the ITU, service providers operating in the State of Qatar may provision such numbers on their networks for use by their customers.

Service providers may also allow inbound roaming for subscribers using international numbers if the appropriate roaming arrangements are in place with the home network operator, subject to the conditions stated in 3.7

IPv6

Usage of IP addresses is very common in IoT ecosystem. Most IoT devices utilize private IP addresses. The CRA encourages IPv6 adoption for IoT in Qatar as a critical initiative. As the demand for IoT devices continues, the existing IPv4 number space faces limitations in addressingthe vast number of devices expected to come online. IPv6, with its virtually limitless address space,is essential for supporting the exponential growth of IoT, enabling seamless connectivity and communication among devices.

In cases where IoT devices require global IP address, IPv6 adoption is vital for ensuring scalability, improved security features, and efficient routing. By promoting IPv6, the CRA aims to foster an innovative ecosystem, enhance Qatar's technological infrastructure, and ensure the nation remains at the forefront of global digital transformation.

CRA supports the adoption of IPv6 by service providers and recommends its implementation. They might be able to offer IoT services on dedicated infrastructure that supports IPv6 (such as having a dedicated P-GW for IoT services) in order to facilitate the early adoption of IPv6.

3.6. SIM Card Registration

Regulation permits Qatari residents to own up to five mobile subscriptions for their devices, which is sufficient for most users and prevents illicit distribution. Service providers are required to verify and record the identities of the owners of SIM cards and eSIMs. However, the CRA understands that the proliferation of IoT devices is likely to mean that individuals will own more than five IoT devices.

Suppliers of IoT devices that provide a subscription service with the device, or a service provider that provides a dedicated IoT subscription plan, associated with a type approved IoT device where the SIM / eSIM cannot be physically removed from the device, will be

exempted from the requirement to limit the number of subscriptions for individuals. It will, however, still be necessary for connectivity providers to validate the identity of their customer, as per the current process.

3.7. Permanent Roaming

Roaming is a well-established principle in mobile telephony. It allows individuals to “roam” on mobile networks in other countries while travelling outside their home country. This is usually attractive for the “visited network” because it brings additional revenue, which accompanies the costs of hosting the in-bound roamer. It should be noted that while roaming for IoT-M services is relatively common, NB-IoT is not at present.

IoT devices often have very low data volumes, often so low that the costs of hosting an in-bound roamer exceed the revenues billed for services. When very large numbers of in-bound IoT roamers exist, this can have a material effect on the operating costs of the visited network and tie up resources that cannot then be used by home subscribers. For this reason, permanent in-bound roaming to Qatar will not normally be permitted, and an IoT device with an IMSI belonging to a network outside the state of Qatar will be automatically blocked from accessing Qatari networks after a period of 90 days if it has attempted to access a Qatari network at least once a week during those 90 days. Once blocked, the IMSI will remain blocked for a further period of 90 days.

Service providers may, at their discretion, permit permanent roaming for commercial reasons, for example, where a bilateral agreement exists.

The CRA defines an IoT device in this context as any IMSI that has attached to a Qatari mobile network but has less than 10 minutes of chargeable voice traffic, less than 10 mobile originated SMS, and less than 200 MB of data in the week under consideration.

A further issue is that devices from Qatar may be taken to other countries and used on foreign networks. The CRA supports such activity provided data sessions are ‘home-routed’, via the subscriber’s home network. Numbers designated for the provision of M2M/IoT services may be used overseas on a temporary basis, to a maximum of thirty (30) calendar days, subject to compliance with the rules and regulations in the overseas jurisdiction in which they are being used (including roaming regulations).

3.8. Consumer Protection

To increase trust and in furtherance of IoT adoption in Qatar, consumer protection is a necessary component in establishing trust and support to consumers and the market as

it develops. We consider the consumer protection aspect should be broken down into two main aspects as follows:

1. Cyber security, data security and privacy.

2. Contractual consumer terms.

Whilst some cybersecurity, data security and privacy are dealt with elsewhere in this position paper, the remainder of this section shall cover the contractual consumer elements.

Current Regulations: CRA Telecommunications Consumer Protection Policy

IoT service providers at each step of the provision of connectivity services shall be required to adhere to existing Telecommunications Consumer Protection Policy and Qatar Consumer Laws as may be updated. These consumer protection measures shall apply to all entities including hardware, service, or connectivity providers when interacting with consumers and such obligations shall apply to any provider no matter if they are established within Qatar or elsewhere.

As a minimum, IoT service providers shall be required to comply with all consumer protection regulations and legislative rules and requirements as set out in the Telecommunications Law (mainly Chapter 10) and the Telecommunications Consumer Protection Policy from the Regulatory Authority Ministry of Information and Communication Technology (ictQATAR), the CRA's predecessor, and all consumer protection policies, guidelines and instruments issued by the CRA (together the **"**Qatar Consumer Laws").

Whilst the National Cyber Security Agency regulates cyber security and data more generally, the CRA may also publish good practices for managing consumer related data privacy requirements for IoT services.

Consumers should be kept informed about the capabilities, limitations and data collection practicesof their IoT devices and services they purchase or use. In line with the CRA's Cloud Policy Framework and other applicable legislation, data storage should be governed as per the regulations and guidelines released by the NCSA and NDPO.

The IoT service provider (if they do collect data about the end users) are not to use the data exceptas permitted or required by the Qatar Consumer Laws, and other applicable legislations.

Consumers should have reasonable control over their personal data. The IoT Service Approval Application shall require, where the personal data processing is necessary for the purpose of operating the IoT connectivity, this should be notified to the consumer at point of initiation.

Liability and Enforcement

Liability for malfunctions or accidents can be complex when interrelated. If necessary, the CRA may issue guidance to clarify responsibilities and liability in the IoT ecosystem. The position is that every IoT service provider is required to provide a contact for notification, and enforcement that will need to be registered in Qatar. This will make enforcement by the CRA easier.

The notification structure would hold each IoT Service Provider as liable for the applicable Qatar Consumer Laws and any other required regulatory elements. Failure by an IoT provider to properly notify the CRA, would be a breach of Qatari law and the CRA has the right to use all relevant enforcement powers. If the CRA fails to take enforcement action, it will duly explain the reasons for such inaction. Decisions by the CRA in relation to IoT shall not be subject to challenge or appeal. As a minimum consumers should be afforded access to an effective complaint and redress mechanisms under the Qatar Consumer Laws in case of issues with IoTproducts and services.

3.9. Data Retention and Data Access

Service providers in Qatar are subject to processes that allow the relevant authorities to carry out lawful investigations that relate to users of Qatar's mobile networks. These apply in the same way to IoT users. Additionally, the CRA requires that providers of public IoT services, and in particular MQTT brokers maintain records (logs) of activity for a period of no less than six months. These shall be made available upon presentation of a lawful request to the relevant authorities. Note, it is not expected that the content of messages be maintained, only the meta-data associated with messages, which might include time and date, location, sending and receiving IP address, device information (such as MAC address or serial number), and associated customer account.

Service providers when handling data will also need to be compliant with the CRA Cloud Policy Framework[2] dated July 2022 regulations and guidelines released by the NCSA and NDPO. This includes the data classification requirements, data localization security,

[2] https://www.cra.gov.qa/en/document/cloud-policy-framework

data interoperability and portability as well as other recommendations. Providers of IoT services may also, in response to a lawful request, be required to cooperate with the authorities in response to an ongoing investigation. This could foreseeably include providing real-time data about specific users. This is especially relevant for threats related to national security.

3.10. Cybersecurity

CRA recognizes that IoT devices have historically employed limited security measures, which has provided threat actors with opportunities for compromising the functions of the IoT devices, accessing personal and sensitive data, and providing entry points for attacks on other systems. Large numbers of IoT devices can be compromised or disabled, or devices operated by key entities can be accessed, threatening Qatar's national security.

The Qatar National Cyber Security Agency publishes various policies, frameworks and guidelines (for example, Qatar Cyber Security Framework 2022 and National Information Assurance Standard)[3]. All suppliers and operators of IoT devices in Qatar must follow the full provisions outlined in such publications.

3.11. Data Security and Privacy

Users of IoT devices have the right to expect that their data is held securely and only used for the stated purposes. Although the definition of data security and privacy does not fall within the remit of the CRA, the relevant guidelines published by the NCSA and NDPO are mandatory regarding data security and privacy. Providers should also refer to the relevant privacy laws with regards to the protection of personal data.

3.12. Interoperability

As the Internet of Things (IoT) ecosystem in Qatar continues to grow, ensuring seamless interoperability among devices, platforms, and services becomes increasingly important. Interoperability refers to the ability of different IoT systems, devices, and networks to work together and exchange data effectively, regardless of the manufacturer, service provider, or technology used.

The CRA recognizes that a lack of interoperability can lead to fragmented ecosystems, increased costs, and reduced efficiency. It can also limit the scalability of IoT solutions and hinder the full realization of the benefits of IoT technologies. To address these

[3] https://www.ncsa.gov.qa/en/regulatory-tools/

challenges, the CRA proposes the following considerations for ensuring interoperability within Qatar's IoT ecosystem:

- **Compliance with Cloud Data Interoperability and Data Portability Regulation:** Where cloud platforms are being used for providing IoT/ M2M services, the CRA expects the service providers to adhere to and comply with the requirements outlined in the Cloud Data Interoperability and Data Portability Regulation published by the CRA[4].

- **Adoption of International Standards:** The CRA encourages the adoption of widely recognized international standards for IoT communication protocols, data formats, and interfaces. This will help ensure that devices and systems from different manufacturers can work together seamlessly and that IoT solutions deployed.

- **Interoperability Testing and Certification:** The CRA may consider establishing a framework for interoperability testing and certification. IoT devices and systems should be tested to ensure they meet these standards before they are approved for use in Qatar. This would involve collaboration with international standards organizations and testing bodies to align Qatar's certification processes with global best practices.

- **Guidelines for Developers and Manufacturers:** The CRA will develop and publish guidelines for IoT developers and manufacturers, emphasizing the importance of designing products with interoperability in mind. These guidelines will include recommendations on the use of standard protocols, data formats, and interfaces to facilitate seamless integration across different platforms and networks.

- **Promoting Open APIs:** The CRA supports the use of open Application Programming Interfaces (APIs) to enable different IoT platforms and services to communicate and exchange data easily. Open APIs can reduce vendor lock-in, encourage innovation, and foster a more competitive market by allowing new entrants to develop interoperable solutions.

- **Stakeholder Collaboration:** The CRA will work closely with stakeholders, including device manufacturers, service providers, and industry associations, to promote

[4] https://www.cra.gov.qa/en/document/regulation-for-cloud-data-interoperability-and-data-portability

interoperability across the IoT ecosystem. Collaborative efforts will focus on developing shared frameworks, best practices, and solutions to common interoperability challenges.

By prioritizing interoperability, the CRA aims to create a more cohesive and efficient IoT ecosystem in Qatar. This will not only enhance the user experience but also support the long-term growth and sustainability of IoT technologies in the country. The CRA invites stakeholders to provide feedback on these proposals and to suggest additional measures that could further promote interoperability within Qatar's IoT landscape.

4 Implementation Strategies

Introduction

IoT is an essential driver of future growth for the IT and telecommunications industries. Approval mechanisms and accountability are critical in establishing a structure for IoT service providers. The CRA's regulatory approach would be designed to support Qatar's IoT market growth. The CRA aims to be flexible in its regulatory approach to align with stakeholders' needs and to create opportunities for commercial IoT development.

Licensing and regulatory oversight by the CRA will need to consider many aspects of the IoT ecosystem, such as spectrum usage, connectivity with telecom networks, and standard terms and pricing for wholesale connectivity. This aims to provide more options in the market for connectivity providers and support the growth of a diverse IoT device market for end-user customers.

4.1. Approval Scheme for IoT Service Provision

Various approaches are used to regulate the provision of IoT services across the globe. A solution that provides adequate information to the CRA and potentially other government authorities as needed, with a flexible and light touch approach on the other hand, is an approach that would create structure while also facilitating rapid growth in Qatar for the industry.

The CRA considers that a simplified IoT Service Approval scheme is appropriate for the current Qatari market landscape to encourage adoption and adopt a light regulatory approach. Depending on the growth of the IoT market, the CRA may consider introducing a class license scheme in the future. The CRA may also collaborate with the Ministry of Commerce and Industries (MOCI) to introduce a new service category for IoT services

and businesses.

On this basis, the CRA will come up with the operational requirements for approval of IoT service provisioning, with a notification requirement to the CRA that would give sufficient oversight while fostering a transparent and efficient system for service providers. All providers of IoT services in Qatar to:

1. appoint a local representative in Qatar; and
2. submit a notification to the CRA with the required details (including those of the local representative) and a brief description of the IoT service.

The service providers shall have to provide the below details (non-exhaustive) as part of their the IoT Service Approval application:

- Eligible use cases for the IoT services being offered
- Spectrum and frequency requirements in line with the CRA's National Frequency Allocation Plan[5]
- Number block requirements
- Equipment approval certificate as subject to the requirements of the CRA's Type Approval regime along with other necessary approvals as outlined in the IoT Service Approval Application (e.g. cyber security assurance certification and common criteria vetting certification from the NCSA)
- Details about the consumer's personal data processing for the purpose of provisioning the IoT connectivity

Such IoT Service Approval would provide structure, information and functionality for the IoT market. Notification as a service provider under the IoT Service Approval and acknowledgement from the CRA would have to be obtained before providing connectivity services.

The CRA shall have a right to require prospective IoT service providers to pay a fee upon notification, update as to change of details, annual fees, and other such communications. The service provider shall be responsible for the costs, expenses, or other financial

[5] https://www.cra.gov.qa/en/document/national-frequency-allocation-plan

commitments arising from the IoT Service Approval Application and the use of their connectivity in line with applicable regulatory obligations.

CRA may consider extending the existing consumer protection regulations and measures to the IoT services.

The CRA will publish further details about the IoT Service Approval Application in due course.

4.2. Pilot programs and sandboxes

Pilot programs and regulatory sandboxes could be instrumental for driving the adoption of emerging technologies in Qatar. They offer significant benefits, such as fostering innovation, ensuring regulatory compliance, boosting economic growth, and enhancing consumer trust. These initiatives are essential for deploying IoT technologies, as they can provide a controlled environment for testing and refining new innovations while ensuring they meet regulatory standards.

It is anticipated that industry will take a lead in the definition of sandboxes. With the CRA's active involvement, the country can effectively leverage these tools to build a dynamic and resilient technological landscape.

4.3. Public-private partnerships

As related to the IoT infrastructure deployment, public-private partnerships can support substantially and leverage resources, share expertise, and ensure that connectivity solutions meet the needs of consumers, businesses, and regulatory bodies alike.

5 Conclusion

The rapid evolution of IoT technologies presents both unprecedented opportunities and significant challenges for Qatar. As the country strides towards its vision of becoming a knowledge-based economy and global digital hub, the integration of IoT into its infrastructure, industries, and everyday life is inevitable and transformative. The key elements of the IoT regulatory framework as outlined in this paper are seen critical in ensuring that the deployment and expansion of IoT technologies in Qatar are conducted in a manner that aligns with national strategic goals, international standards, and the well-being of its citizens.

By establishing a forward-looking and flexible regulatory environment, CRA aims to foster

innovation while safeguarding the interests of all stakeholders. This includes promoting competition, ensuring the security and privacy of data, protecting consumers, and maintaining the integrity of Qatar's telecommunications infrastructure. The proposed IoT regulatory framework is designed to be both comprehensive and adaptive, addressing current needs while being sufficiently robust to accommodate future technological advancements.

The CRA recognizes that IoT is not just a technological innovation; it is a catalyst for economic diversification, environmental sustainability, improved quality of life and stimulating investment, both local and foreign. As such, the CRA is committed to working collaboratively with all stakeholders, including government entities, private sector players, and the wider community, to implement this regulatory framework effectively.

Moreover, by encouraging public-private partnerships, supporting pilot programs and regulatory sandboxes, and ensuring clear and enforceable guidelines, Qatar is positioning itself as a leader in the global IoT landscape. The CRA's proactive approach to regulation aims to create an environment where IoT can thrive, driving progress towards Qatar's national development goals.

In conclusion, the CRA's strategic vision for IoT regulation in Qatar is both ambitious and necessary. It is designed to harness the full potential of IoT technologies, ensuring that their deployment contributes positively to the nation's development while mitigating any associated risks. As the regulatory framework evolves, the CRA will continue to engage with stakeholders to refine and adapt its approach, ensuring that Qatar remains at the forefront of technological innovation and regulatory best practices.

6 Annexure I: Technical Standards

6.1. Network and equipment

Associated specifications

The following unattached international and/ or national standards shall be applied, and deemed to be an integral part of this Specification:

- Type Approval Policy 2009
- Type Approval Guidelines 2011
- Short Range Devices as per Class License for Short Range Devices (SRD)

- Qatar National Frequency Allocation Plan and Specific Assignments
- Radio Spectrum Policy
- General Guidelines for Radio Spectrum Licensing
- Guidelines For Managing Spectrum Interference
- ETSI EN 301 893: Broadband Radio Access Networks
- ITU-T Y.2060: Overview of the Internet of Things

Technical Requirements

Designing IoT networks involves navigating several challenges to ensure optimal performance across various applications. Essential considerations include low-latency communication for real-time responsiveness. Strategies such as edge computing, auto-provisioning, and network segmentation play a vital role in enhancing resilience, security, and efficiency while also addressing environmental sustainability in IoT implementations. Listed below are the baseline technical requirements for IoT networks and equipment. It is important to note that not all requirements may be deemed applicable for all universally; and its relevance would be determined by specific use cases or evaluated on a case-by-case basis:

- Support for low-latency communication: IoT devices are recommended to be designed for real-time operations and optimized for low-latency communications. Technologies such as URLLC (Ultra-Reliable Low Latency Communication) should be considered, especially for critical IoT applications like healthcare and autonomous vehicles.
- Bandwidth allocation: It is advisable to use traffic prioritization mechanisms, such as QoS (Quality of Service), to prioritize critical IoT applications over non-essential traffic, ensuring reliable performance even under high-load conditions.
- Multi-protocol support: IoT equipment is encouraged to support LTE (4G), NB-IoT, or LTE-M as a minimum, with additional support for diverse communication protocols such as Wi-Fi, ZigBee, LoRaWAN, NB-IoT, and 5G. This flexibility allows deployment to be tailored based on application-specific needs such as range, power consumption, and bandwidth.
- Edge computing integration: IoT networks are recommended to be designed with

edge computing in mind, enabling critical processing to be offloaded to edge devices. This approach can help reduce latency, enhance resilience, and minimize data transmission to the central cloud.

- Auto-provisioning: It is recommended to enable automatic discovery and provisioning of IoT devices to reduce manual intervention. Secure onboarding processes, such as certificate-based mutual authentication, should be considered to enhance security.
- Network segmentation: To enhance security, consider logically or physically separating IoT devices from sensitive corporate systems. Approaches like VLANs, firewalls, or Software Defined Networking (SDN) can be utilized to minimize the risk of lateral movement in case of a breach.
- Sustainable manufacturing and operations: It is advisable to implement measures that minimize the environmental impact of IoT deployments. This may include sustainable manufacturing practices and planning for the recycling of IoT equipment where feasible.
- Resilient network design: Designing the IoT network with resilience in mind is highly recommended to ensure continuous operation. Incorporate redundancy mechanisms such as multi-homing, failover links, and mesh network architectures to achieve high availability.
- RF spectrum efficiency: For IoT networks that rely on wireless communication, adherence to the CRA's applicable regulatory frameworks is crucial to ensure the efficient use of RF spectrum. Techniques such as frequency hopping and channel bonding should be implemented, where applicable, to minimize interference with other communication services. Service providers are required to comply with the most recent National Frequency Allocation Plan issued by the CRA, including any future revisions or updates.

Additional references:

- IEEE 802.11: Wireless LAN Standards
- 3GPP TS 23.501: System Architecture for the 5G System

6.2. IoT identifiers

Associated specifications

The following unattached international and/ or national standards shall be applied, and

deemed to be an integral part of this Specification:

- CRA National Numbering Plan
- CRA Numbering Regulation
- ETSI TS 103 306: Machine-to-Machine Communications (M2M) Identification Requirements
- ITU-T Y.2066: Common Requirements of IoT

Technical Requirements

IoT identifiers, such as IP addresses and MAC addresses, are essential for managing and tracking connected devices. Standardizing these identifiers is crucial for uniform protocols, device compatibility, robust security, facilitating innovation and scalability across industries. The baseline technical requirements for IoT identifiers are listed below.:

- Persistent unique identifiers (UID): It is recommended that each IoT device possess a globally unique identifier (GUID or EUI-64) that remains persistent throughout its lifecycle. This ensures consistent tracking across different network domains. Device identifiers should avoid containing or being derived from personally identifiable information, and manufacturers are encouraged to implement measures to prevent tampering or spoofing of these identifiers.
- Dynamic identifier allocation: IoT platforms should support dynamic identifier allocation through protocols like DHCP. Mechanisms for resolving identifier conflicts should be incorporated to ensure seamless operation.
- Support for multiple identifier schemes: Systems are advised to support a variety of identifier schemes (e.g., IP addresses, MAC addresses, EUI-48/64, URIs) to accommodate the diversity of IoT devices and protocols. Ensuring identifiers are independent of specific network technologies or service providers is recommended to enhance flexibility and avoid vendor lock-in.
- Hierarchical identifier structure: Adopting a hierarchical structure for IoT identifiers is suggested to support scalability. Identifiers could include elements reflecting device type, manufacturer, location, and operational status, simplifying management in large-scale deployments.

- Device attestation: Device attestation mechanisms are recommended during onboarding to verify the legitimacy of devices claiming an identifier. Methods like Trusted Platform Modules (TPMs) or Secure Elements (SEs) can be employed for secure boot and identifier verification.
- Self-verifying identifiers: It is advisable to adopt self-verifying identifiers, such as cryptographic hash-based identifiers, to enable authentication without relying on centralized databases. This approach can enhance both scalability and security.
- IoT identifier management system: Implementing centralized IoT identifier management systems is recommended to track device lifecycle events, including provisioning, updates, and decommissioning. Mechanisms like ID registries can help resolve identifiers across distributed deployments. The processes for identifier assignment and management should be efficient to minimize latency and ensure timely device identification.

Additional references:

- ISO/IEC 29182: Sensor Network Identifier (ID) Architecture

6.3. Interoperability

Associated specifications

The following unattached international and/ or national standards shall be applied, and deemed to be an integral part of this Specification:

- CRA Regulation for Cloud Data Interoperability and Data Portability
- TASMU Interoperability Policy

Technical Requirements

Interoperability is vital in IoT for seamless communication and integration across diverse vendors. To avoid vendor lock-in, devices should support multiple vendors and adhere to open standards. Cross-domain interoperability and semantic frameworks ensure consistent data exchange. Protocol translation, middleware solutions, cross-platform tools, and standardized APIs simplify integration, while recognized network technologies and security protocols enhance flexibility and resilience. The baseline technical requirements for interoperability are listed below. It is important to note that not all

requirements may be deemed applicable for all universally; and its relevance would be determined by specific use cases or evaluated on a case-by-case basis:

- Multi-vendor support: It is recommended that IoT devices be tested and certified for interoperability with products from other vendors to avoid vendor lock-in. Adopting open standards, such as MQTT and OPC UA, is encouraged to ensure seamless multi-vendor interoperability. IoT equipment manufacturers and service providers should provide comprehensive documentation detailing their devices' interoperability features and supported protocols.
- Cross-domain interoperability: IoT systems are advised to enable interoperability across devices from different verticals, such as healthcare, transportation, and smart homes, by adhering to cross-domain standards like ISO/IEC 30141 (IoT Reference Architecture).
- Semantic interoperability: Employing semantic frameworks, such as OneM2M and W3C WoT, is recommended to define shared vocabularies and ontologies. This ensures consistent data interpretation and action between devices from different manufacturers. For internet-connected IoT devices, supporting IPv6 is essential, while maintaining IPv4 compatibility is suggested for backward compatibility.
- Protocol translation gateways: Consider using protocol translation gateways to facilitate communication between IoT devices operating on different protocols, such as MQTT, CoAP, HTTP, and LWM2M.
- Middleware for IoT orchestration: Middleware solutions are recommended to abstract the complexities of underlying network and hardware layers. This enables smooth orchestration of IoT services, seamless integration with existing IT systems, and collaboration across various IoT platforms.
- Cross-platform SDKs: Device manufacturers are encouraged to provide cross-platform Software Development Kits (SDKs) to simplify integration across diverse hardware, middleware, and cloud platforms, thereby reducing dependency on specific vendors.
- Firmware and software abstraction: It is advisable to implement standardized APIs that provide abstraction layers for firmware and software services. This enables unified management and control of IoT devices from different manufacturers through a single platform.

- IoT equipment should be designed to support widely recognized network technologies, enabling flexibility for different deployment scenarios.
  - Wi-SUN (Smart Utility Network)
  - Bluetooth Low Energy (BLE)
  - Zigbee
  - Zwave
  - LoRaWAN
  - NB-IoT
  - LTE-M
  - 4G/5G
- IoT equipment is recommended to support widely recognized and standardized data formats to ensure seamless information exchange across diverse systems and platforms, such as:
  - JSON
  - XML
  - CBOR
- IoT equipment should adhere to widely recognized security protocols to safeguard information exchange and ensure secure communication, such as:
  - TLS 1.2 or higher for data in transit
  - XML OAuth 2.0 for authorization
  - MQTT with TLS for publish/subscribe messaging
- IoT platforms and devices are encouraged to expose well-documented APIs to facilitate integration with other systems and applications. Adherence to industry-standard API specifications, such as RESTful APIs, is advised to enhance compatibility and ease of use.
- IoT platforms should provide mechanisms to enable seamless data exchange with different IoT platforms and cloud service providers in Qatar, fostering interoperability and collaboration.

Additional references:

- ISO/IEC 21823 Interoperability for IoT systems standards
- ETSI TR 103 536 interoperability standards
- ISO/IEC 30141: Internet of Things Reference Architecture
- Wi-Fi (IEEE 802.11 in 2.4 GHz, 5 GHz, and 6 GHz frequency bands)

- IEEE 802.11ah-based Wi-Fi HaLow
- IEEE 802.15.4-based Ultra-Wideband (UWB)

6.4. Data Access and Retention

Associated specifications

The following unattached international and/ or national standards shall be applied, and deemed to be an integral part of this Specification:

- CRA Cloud Policy Framework
- Qatar NCSA National Data Classification Policy
- Law No.13 of 2016 Qatar Personal Data Privacy Protection Law
- Qatar National Information Assurance Standard
- ITU-T Y.2068: Functional Framework for IoT Data Access

Technical Requirements

Effective data lifecycle management is essential for the safe and legal handling of IoT-generated data. This involves implementing multi-layered access restrictions, tier-based storage, and retention policies, ensuring prompt data erasure requests, maintaining record integrity with immutable formats, and providing real-time access to authorities for improved data management. The baseline technical requirements for data access and retention are listed below. It is important to note that not all requirements may be deemed applicable for all universally; and its relevance would be determined by specific use cases or evaluated on a case-by-case basis:

- Data lifecycle management: It is recommended to define clear data lifecycle policies for IoT-generated data. These policies should establish retention periods based on data types (e.g., sensor data, user interaction logs) and align with legal or regulatory requirements.
- Hierarchical data storage: Adopting a tiered storage architecture (hot, warm, cold storage) is suggested to balance cost and performance. Frequently accessed data can be stored in faster, higher-cost tiers, while historical or less frequently accessed data can be archived to more economical storage solutions.

- Access control layers: Multi-layered access control mechanisms are advised to safeguard sensitive IoT data. Employ fine-grained access controls at file, network, and application levels to enhance security.
- Data obfuscation and anonymization: Techniques such as data obfuscation, tokenization, or anonymization are recommended before archiving or sharing IoT data. These measures can protect user privacy while maintaining the utility of data for analytics and decision-making.
- On-demand data deletion: Providing users with mechanisms to request immediate deletion of personal or sensitive IoT data from active databases and backup systems is encouraged to ensure compliance with data protection regulations.
- Data locality management: It is recommended to specify the physical or virtual locations of IoT data storage to align with regional data sovereignty laws. Dynamic storage solutions that can adapt to evolving legal and operational requirements should also be considered.
- Immutable data records: Storing critical IoT data in immutable formats, such as WORM (Write Once Read Many storage), is advisable to ensure compliance and support audit requirements. Including mechanisms for real-time and historical audit trails is recommended to enhance compliance with applicable regulations.
- Adopting data classification practices in accordance with the Qatar NCSA National Data Classification Policy is suggested to ensure proper handling and security of different data types.
- It is encouraged to implement data minimization practices, collecting and retaining only the data necessary for its intended purpose to reduce storage overhead and enhance privacy.
- Providing clear and transparent information about how and why personal data is processed is recommended. Include details of the entities responsible for collecting and processing the data.
- Establishing specific retention periods for different types of IoT data is advisable to maintain compliance with regulatory standards. Ensure these retention periods are consistently followed.
- Implementing secure and reliable data deletion processes is suggested for ensuring privacy and compliance once the defined retention periods have expired.

- Maintaining a comprehensive inventory of all collected and stored data is recommended to facilitate effective data governance and compliance efforts.
- Using role-based access controls is advised to ensure that data access is limited to authorized users and systems, improving security.
- Keeping a detailed activity log that captures critical metadata, including timestamps, IP addresses, device information, and account numbers, for a period of at least six months is recommended.
- It is advisable to ensure that activity logs are readily accessible to relevant authorities to support law enforcement and investigative efforts when required.
- Providing authorized authorities with real-time access to data about the network, users, and equipment is recommended to enable effective responses to national security threats.

Additional references:

- ETSI TS 103 645: IoT Data Access and Privacy

6.5. Cybersecurity

Associated Specifications

The following unattached international and/ or national standards shall be applied, and deemed to be an integral part of this Specification:

- Qatar Cyber Security Framework 2022
- Qatar National Information Assurance Standard
- Law No.13 of 2016 Qatar Personal Data Privacy Protection Law
- Qatar Cybercrime Prevention Law
- ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27400

Technical Requirements

The cybersecurity domain evolves with pace within the IoT ecosystem. Whilst it is not possible to list all the cybersecurity requirements, below is a list of essential baseline requirements to be considered. Additionally, IoT service providers and device manufacturers should regularly perform security risk assessments and threat modelling

to enhance their products and IoT services security posture. Given below are the baseline technical requirements for cyber security. It is important to note that not all requirements may be deemed applicable for all universally; and its relevance would be determined by specific use cases or evaluated on a case-by-case basis:

- No Default Passwords: IoT devices are recommended to use unique passwords by default or allow users to define their own. Avoid the use of default, hard-coded credentials to enhance security.
- Secure Credential Storage: Sensitive information such as passwords, API keys, or cryptographic keys should be securely stored using encryption or other protective mechanisms. Multi-factor authentication (MFA) is recommended for critical IoT devices, applications, and services to strengthen security.
- Software Updates and Patch Management: IoT devices should support secure, timely, and automatic software updates throughout their lifecycle, including mechanisms to address security vulnerabilities promptly.
- Default Configuration Security: It is recommended to prioritize security in the default configurations of IoT devices and services by disabling features that are not essential to their core functionality.
- Secure Device Set-Up: IoT manufacturers are encouraged to provide clear and user-friendly guidance for end-users on securely setting up IoT devices, ensuring ease of understanding and proper configuration.
- Input Data Validation: IoT systems are advised to validate all data inputs, whether from user interfaces, APIs, or inter-network communications, to ensure only verified and trustworthy data is processed.
- Resilient System Design: IoT devices and services are advised to incorporate resilience features to handle network or power outages effectively, minimizing disruption.
- Attack Surface Minimization: Reducing the attack surface is essential. Disabling unused network and logical interfaces, along with implementing secure development practices, is recommended to enhance the security of IoT software components.
- Logging and Monitoring Comprehensive logging and monitoring systems should be implemented to track IoT device activity, monitor network performance, and observe application behavior. Alerts for errors or anomalies can help improve

incident response.

- Physical Security (Hardening): IoT devices deployed in public or high-risk locations are recommended to be tamper-resistant and designed to withstand physical attacks. This reduces the risk of unauthorized access or theft.
- Fail-Safe Modes: Safety-critical IoT devices should include fail-safe modes to automatically switch to a secure state in cases of malfunction, network issues, or power failures.
- Secure Communication: Employing best-practice cryptographic methods is advised to ensure secure communication, maintaining both the confidentiality and integrity of transmitted data.
- Security Audits: Conducting periodic security audits and assessments is recommended to proactively identify vulnerabilities in IoT devices, platforms, and data storage systems.
- End-of-Life Management: Establishing clear end-of-life policies for IoT devices that are no longer capable of receiving secure updates is advisable. These devices should be safely decommissioned or replaced to prevent potential risks.
- Access Control: Role-based access control (RBAC) and the principle of least privilege should be implemented to limit access to sensitive data and functions strictly to authorized users and systems.
- Device Identity Management: Each IoT device should have a unique and verifiable identity. Device authentication mechanisms are recommended to ensure that only legitimate devices are connected to the network.
- Secure Decommissioning: Securely wiping all sensitive data and configurations before decommissioning or transferring IoT devices is recommended to protect user information and prevent misuse.
- Supply Chain Security: Enhancing security across the IoT device supply chain, including secure manufacturing practices and tamper-evident packaging, is encouraged to mitigate risks of compromise during production or delivery.
- Anomaly Detection: Implementing real-time anomaly detection systems is recommended to monitor IoT device behavior and quickly identify deviations that could indicate security issues.

Additional references:

- ETSI EN 303 645 Cybersecurity standard for consumer IoT

6.6. Data security and privacy

Associated Specifications

The following unattached international and/ or national standards shall be applied, and deemed to be an integral part of this Specification:

- Law No.13 of 2016 Qatar Personal Data Privacy Protection Law
- Qatar Cyber Security Framework 2022
- Qatar National Information Assurance Standard
- ISO/IEC 27001, ISO/IEC 27002, ISO 27018 and ISO/IEC 27400

Technical Requirements

To ensure the security and privacy of IoT services, providers must follow guidelines from Qatar's National Cyber Security Agency and National Data Privacy Office. This includes integrating privacy protections from the start, using encryption, obtaining user consent, and having clear protocols for data breaches and secure data disposal. Given below are the baseline requirements for data security and privacy. It is important to note that not all requirements may be deemed applicable for all universally; and its relevance would be determined by specific use cases or evaluated on a case-by-case basis:

- Service providers are encouraged to follow all relevant guidelines published by the Qatar National Cyber Security Agency and the National Data Privacy Office to ensure adherence to local security and privacy standards.
- Privacy protection mechanisms should be integrated into the early stages of IoT device and service design. This ensures that personal data is collected and processed in accordance with relevant data protection regulations.
- Data encryption: It is recommended to apply industry-standard encryption mechanisms (e.g., AES-256) to IoT data, both in transit and at rest, to ensure the confidentiality and integrity of sensitive information.
- User consent mechanisms IoT devices should incorporate mechanisms to obtain

and document user consent for data collection, ensuring transparency and compliance with privacy regulations.

- Anonymization and pseudonymization: When applicable, personally identifiable information (PII) should be anonymized or pseudonymized in accordance with data protection regulations to protect user privacy.
- Data breach protocols: Service providers should establish documented processes for notifying stakeholders in the event of a data breach, ensuring prompt communication and appropriate action.
- End-of-life data management: At the end of their lifecycle, IoT devices should securely erase any retained data to prevent unauthorized access or misuse after decommissioning.

7 Annexure II: IoT Landscape

7.1. IoT Ecosystem and Value Chain

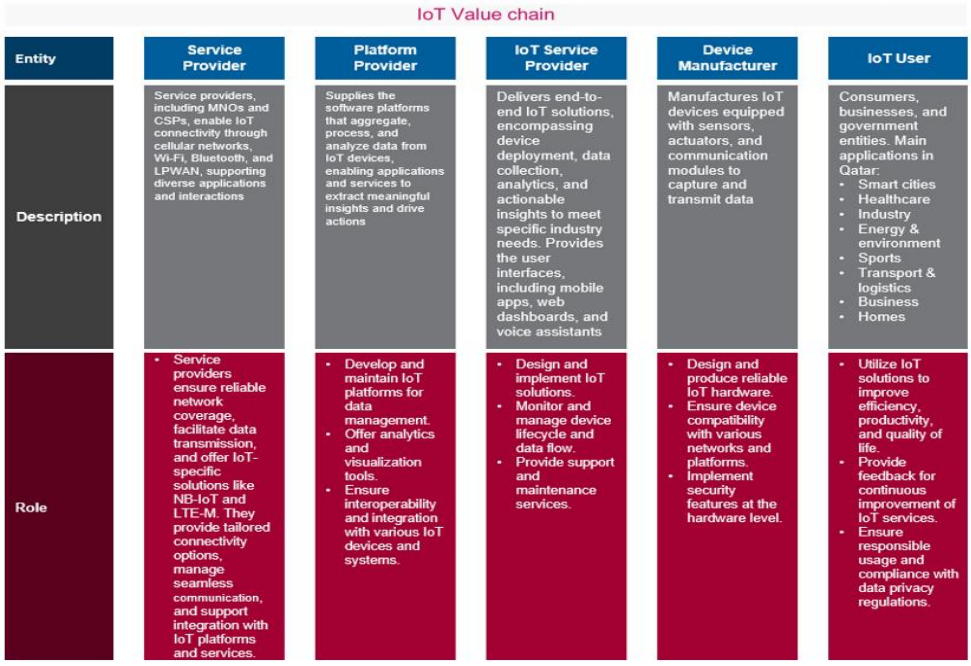
The IoT ecosystem encompasses a vast and intricate network of interconnected devices, systems, and services that work together to collect, analyze, and act upon data. These devices range from simple sensors to complex machinery, all capable of communicating with each other and with central systems over the internet. The IoT ecosystem includes several key components:

1. **Devices/Sensors:** The physical objects equipped with sensors that gather data.
2. **Connectivity:** The communication networks that link devices, including cellular, Wi-Fi, Bluetooth, and other wireless technologies.
3. **Data Processing:** The infrastructure and software used to process and analyze data collected from IoT devices.
4. **Platforms:** The operating systems required for aspects such as ECO provisioning, billing, application development, device and customer service management.
5. **User Interface:** The applications and interfaces through which users interact with IoT devices and data.
6. **Security:** The measures in place to protect IoT devices and data from cyber

threats and unauthorized access.

The various entities that make up the ecosystem and their roles are shown in the value chain in Figure 1 below. Note that the three entities (service provider, platform provider and IoT service provider) may be aggregated together as one or two entities. This means that a single entity may offer connectivity services, operating processes and sector specific applications.

Figure 1: IoT Value Chain: Key Players and Roles



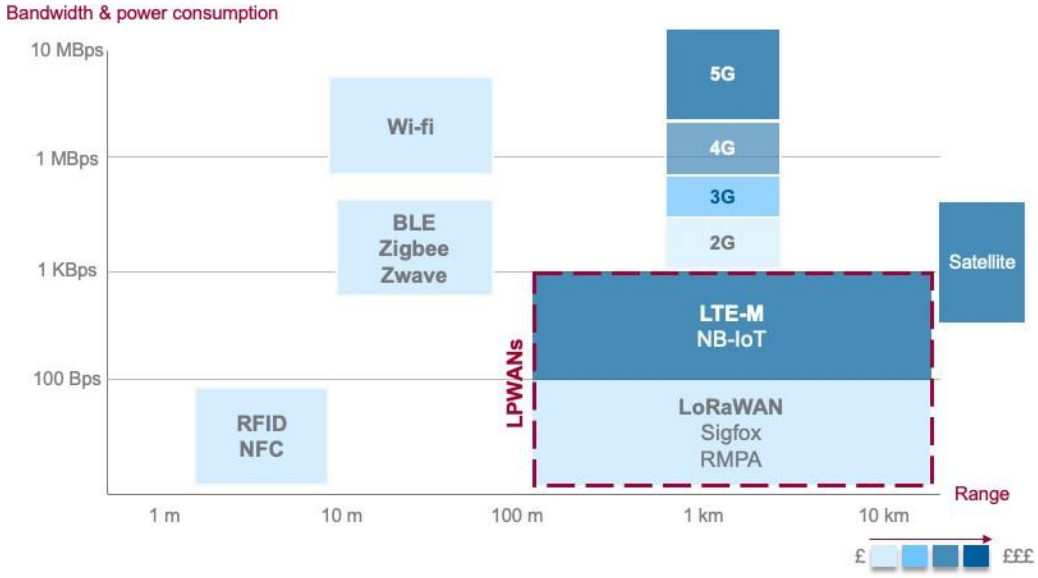
7.2. Technologies for IoT Connectivity

An IoT service depends largely on the ability of IoT devices to communicate with each other, together with cloud-based services availability. Typically, these are based on wireless technologies, and a wide number of standards exist to facilitate this. The choice of radio technology generally depends upon the goals of the application,and there are usually trade-offs between communications speed, distance and power utilization. This is shown in figure 2.

Wireless devices function within specific frequency bands, which are regulated and allocated by the regulatory authorities of each country. Service providers are allocated licensed spectrum to deliver IoT services using technologies like LTE/5G, NB-IoT, and LTE-M. In addition, unlicensed spectrum may also be used for private IoT networks in some instances. For example, frequency bands such as 2.4 GHz, 5 GHz, and 6 GHz

(commonly used for Wi-Fi), along with the 433 MHz UHF band for low-power devices, can support IoT networks like LoRaWAN.

Figure 2: Map of Radio Technologies Against Bandwidth and Range



Although desirable, radio connectivity cannot be assumed to be fundamentally reliable. As IoT devices can move around, they may be also out of contact or switched off / disconnected frompower. The MQTT messaging protocol has emerged to address this challenge. In this case, messages from and to IoT devices may be queued in the event that they are not immediately available, so as to ensure that messages are not lost.

LoRa, Z-Wave, and Zigbee are radio-based technologies that provide low-power, efficient, short-range communications and are especially suitable for small, low-cost devices. These technologies enable many IoT applications, from smart home devices to industrial sensors.

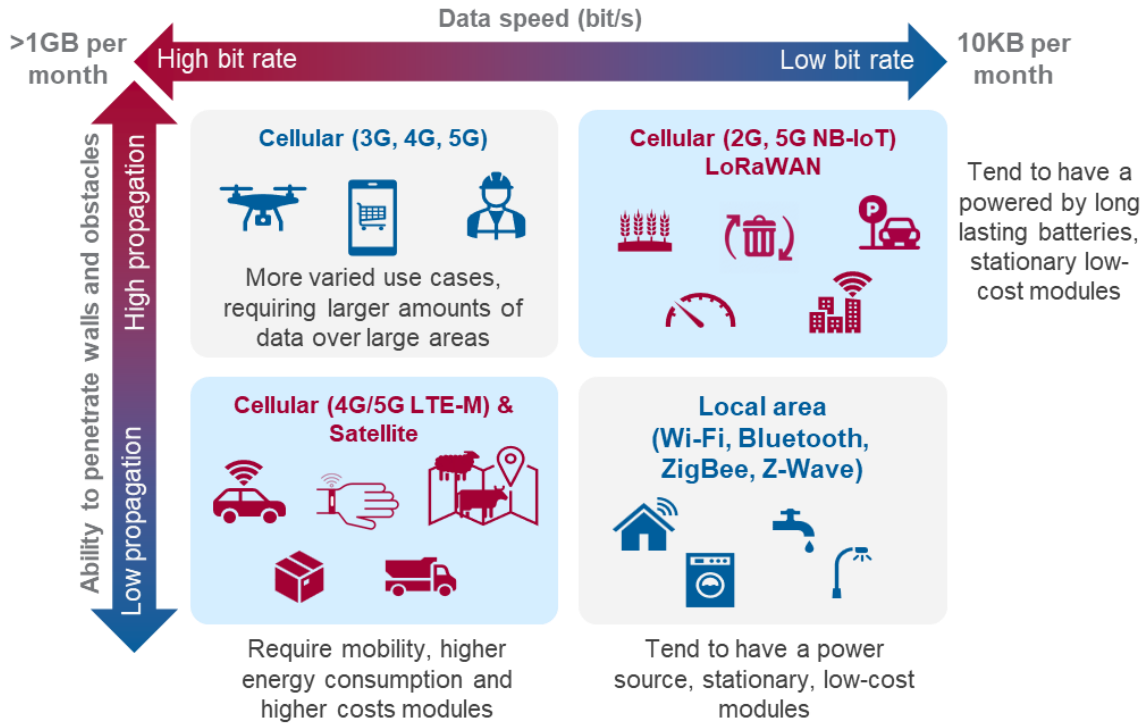
LoRaWAN and NB-IoT are designed to provide long-range communication and low power consumption, each with strengths and ideal use cases. LoRaWAN is often chosen for scenarios where cost and flexibility are critical. It operates in the unlicensed spectrum, making it a cost-effective solution for many applications. Whereas NB-IoT is preferred for applications that require high reliability and operate within the licensed spectrum of cellular networks. It offers robust connectivity, making it suitable for critical applications.

LoRaWAN and NB-IoT are leading LPWAN technologies, each offering unique benefits for various IoT applications. They play a significant role in developing sustainable and efficient IoT ecosystems, supporting environmental sustainability goals and enhancing

the quality of life through more competent resource management.

The type of technology utilized in IoT use cases is summarized in the chart below, which highlights that the technology is dependent on the need to penetrate walls and obstacles (propagation) and the bandwidth / speed required.

Figure 3: IoT Connectivity Types Based on Speed and Propagation



7.3. IoT and the Environment

The Environmental Impact and Need for Proper Disposal Policies

Lithium batteries, vital to IoT applications for their efficiency and reliability, pose significant environmental risks if improperly disposed of. They can contaminate soil and water with hazardous materials like lithium and cobalt and even become fire hazards if mishandled at the end of their life cycle.

To effectively address these challenges, the following responsible disposal practices are recommended:

Recycling Centers: *Drop off used batteries at designated recycling facilities.*

Authorized Collection Points: *Utilize electronic waste collection programs offered by retailers and service providers.*

Special Disposal Containers: *Use battery-specific disposal bins in public spaces like malls and schools.*

Follow Local Regulations: *Adhere to local regulations and guidelines issued by the Ministry.*

By fostering recycling programs, raising awareness, and advocating for manufacturer responsibility, these initiatives aim to reduce the environmental impact of lithium batteries and support sustainable IoT growth.

7.4. IoT Global Trends

Several trends are emerging that impact IoT adoption. These may be summarized as:

- **Falling Costs** - Falling IoT device and subscription costs, driven by competition and technological advances, expand adoption and use cases.
- **Value Added Services** – Industry-specific services cater to sectors like smart cities, healthcare, and industrial IoT.
- **Data-Driven Value** - AI and analytics unlock IoT's potential through smarter platforms and predictive solutions.
- **Security Focus** - Robust hardware, software, and cloud-based security solutions address rising risks.
- **Cloud Platforms -** Ecosystems like AWS IoT and Azure IoT centralize management and analytics.
- **Industry 4.0 -** IoT automates processes, enabling real-time monitoring and advanced analytics.
- **Converged Connectivity –** Hybrid cellular-satellite solutions, including emerging D2D services, enhance IoT applications.

7.5. Use Cases

The IoT ecosystem encompasses a variety of established use cases but also needs to be able to adapt to new ones that may arise. The TASMU platform, managed by MCIT, is one of the key entities enabling various IoT use cases across industry sectors. The CRA's analysis has identified the following use cases relevant to Qatar, primarily based

on references to TASMU's initiatives.

Figure 4: Use Cases of Particular Relevance to Qatar

Connected Cities	Connected Healthcare	Connected Industry	Connected energy & environment	Connected Sports	Transport & Logistics	Connected business	Connected homes
Public transport	Connected HealthTech wearables	Agriculture + animal tracking	Smart metering	Fitness trackers	In-vehicle emergency call system	Alarms + alerts	Alarms + alerts
Environment & public safety	Clinical remote monitoring	Drones/aviation	Real time performance monitoring	Wearables	Cargo and asset tracking	Smart buildings	Smart buildings
Smart lighting	Assisted living	Fuel management	Smart grid & distribution	VT & AR experiences	Fleet management	CCTV	Household devices
Road traffic management	Telemedicine	Mining and Oil&Gas	Environment and weather monitoring	Connected fitness equipment	Roadside assistance	Networked equipment	Connected appliances
Smart parking	Hospital appointment scheduling	Automotive	Waste reduction, conservation, and sustainability goals	Smart stadiums	Usage based insurance	Office equipment	
Resilient energy and infrastructure		Lone worker security	Pipeline monitoring in oil & gas		Vehicle diagnostics	Asset tracking	
Drone management		Logistics, warehousing & storage			Vehicle navigation	Retail	
Local information provision		Manufacturing			Autonomous vehicle management		

8 Annexure III: Qatar IoT Landscape Issues and Challenges

As eluded in section 2.3 of this document, the research carried out among stakeholders in the State of Qatar that have helped CRA to identify areas that may require regulatory intervention are further detailed below along with a summary of CRA's position against each of them.

S. No.	Issues and Challenges	CRA's Position
1.	**IoT Identifier** IoT adoption is limited by a 5-SIM cap for expats and the lack of smaller, cost-effective number blocks (100–1000) for service providers, who currently face high allocation thresholds.	CRA may consider revising the current limit/restriction on the number of SIMs per customer for IoT specific services. The CRA's position to maintain the current number block allocation scheme. If required, the CRA will review and incorporate changes based on the market needs in the future.

	Non-telecom IoT providers face regulatory gaps, with SIM usage required to align with Consumer Registration Policy and MOI rules.	
2.	**Equipment** To ensure that IoT infrastructure and solutions are fit for future use, stakeholders believe that it would be useful to mandate Dual-stack IPv4/6 standard on all new/imported IoT devices and deployments. The lack of clear guidance on Service Providers and customer responsibilities for uncertified devices purchased without equipment and the need for interoperability standards to ensure seamless communication between devices from different manufacturers.	The use of IPv6 is encouraged. However, CRA also considers that the use of dual-stack IoT devices is suited to the current market landscape and implemented use-cases.
3.	**Roaming** Service providers highlight the need for CRA guidance on permanent roaming to enable seamless international IoT connectivity. They also emphasize removing limits on outbound roaming for Qatari IoT SIMs while restricting inbound roaming for foreign IoT SIMs to support a sustainable local IoT industry.	CRA recommends that for in-bound roaming and international IoT SIMs, the usage shall be capped to 90 days, unless an appropriate bilateral agreement exists between the service providers. For the local IoT service providers, it is recommended to use the allocated number ranges for their respective IoT services. No portability or roaming shall be permitted for such cases.

4.	**Interoperability** Challenges in integrating IoT technologies across diverse sectors stem from unique operational needs and complex system architectures, requiring collaborative frameworks tailored to specific industries. Additionally, the lack of clear regulations in Qatar's IoT sector allows low-quality imported devices, causing issues with interoperability, service quality, and security.	CRA encourages adoption of globally recognized standards for IoT devices being imported and used in Qatar. The CRA may consider establishing a framework for interoperability testing and certification in collaboration with the other regulatory bodies or sector regulators.
5.	**Spectrum Management** While the current spectrum plan is deemed sufficient, there is a consensus among entities that a review may become necessary should there be a surge in use cases within the country.	CRA is currently reviewing the Spectrum Plan / National Frequency Allocation Plan. A public consultation will be conducted to obtain feedback from the stakeholders. CRA has also established a Class License for Short-Range Devices, the latest updated version (published in December 2024) can be referred to on the CRA's website.
6.	**IoT Services Licensing and Regulation** The lack of clear IoT guidelines and standards in Qatar, including licensing schemes, spectrum allocation, and security measures, creates challenges for adoption and quality assurance. Coordinating with multiple agencies for IoT-related	CRA may consider implementing an authorization or notification scheme for approval of IoT services. Further, CRA may in collaboration with the Ministry of Commerce and Industries (MOCI), introduce a new services segment for IoT. Details of the same shall be published in due course.

	licenses adds complexity, while stakeholders believe light yet clear regulations would encourage collaboration, integration, and support for region-specific IoT solutions.	Depending on the IoT market growth in the coming years, CRA may consider issuing a class license for IoT services if needed.
7.	**Governance and Coordination with Stakeholders** The complexity of IoT environments, with multiple stakeholders and unclear governance, calls for a collaborative forum or committee to address interdisciplinary challenges and support service providers. Additionally, collaboration between multiple agencies and the CRA is needed to clarify requirements for IoT services, particularly in areas like healthcare and public safety.	CRA will adopt a light-touch regulatory approach towards IoT. For example, introducing simplified approval and notification processes, establishing IoT Advisory Committee, in collaboration with other entities.
8.	**Cost of Technology and Budget Constrains** High costs in developing IoT solutions are driven by the limited scale of initiatives, the lack of specific budgets for IoT (often absorbed into overall IT budgets), and the significant expense of connectivity for IoT applications.	CRA believes that as the market matures, the cost of technology and implementation for IoT services will gradually reduce. CRA also recommends the organizations in Qatar to include IoT as part of their overall strategy and budget-planning to realize the potential benefits of this technology.
9.	**Skills Gap and User Awareness** The continuous evolution of IoT technologies, coupled with a shortage of skilled professionals, makes it challenging for entities in	CRA may consider collaborating with other organizations, industry experts and academic institutions to promote trainings

	Qatar to design, implement, and maintain IoT solutions. A lack of user awareness about IoT risks, opportunities, and use cases further hampers adoption, highlighting the need for CRA's guidance in expertise development, capacity building, and promoting IoT best practices.	and upskilling of professionals in the IoT domain.
10.	**Data Management** The lack of robust IoT data portability guidance risks vendor lock-in, while restricted cross-border data flow limits IoT's potential. Although past challenges arose from providers storing data outside Qatar, the recent Cloud Policy addresses these issues, enabling greater flexibility and compliance in data management.	CRA recommends adhering to the relevant regulations and policies published by the NCSA, NDPO and other sector regulators to implement the appropriate controls within their IoT environment.
11.	**Data Privacy** With the increase in IoT devices and systems collecting and transmitting large volumes of personal and sensitive data, ensuring data privacy is a significant concern. Stakeholders believe that measures should be defined to secure the data being collected and processed by IoT devices and service providers.	The CRA advises following regulations and policies issued by the NCSA, NDPO, and other sector regulators to ensure appropriate controls within IoT environments.
12.	**Security and Resilience** Some IoT systems, such as those in healthcare, transportation, and industrial operations, may be critical	The CRA advises compliance with regulations and policies issued by the NCSA, NDPO, and other sector regulators to

	for customer safety. However, there is limited awareness and clarity around the measures and controls required to ensure the security, resilience, and availability of critical IoT services.	ensure proper controls within IoT environments. Additionally, the CRA may work with these regulatory bodies to create sector-specific guidelines for IoT service usage.
13.	**Consumer Protection and Liability** Consumers lack adequate information about IoT devices' capabilities, limitations, and data practices, as well as effective complaint and redressal mechanisms. Stakeholders seek consumer protection measures across the value chain, including platform providers and manufacturers, even when these entities operate outside the jurisdiction. Additionally, there is unclear liability and responsibility for malfunctions or accidents involving interconnected IoT devices.	CRA may consider extending the existing consumer protection regulations and measures to the IoT services. Further details of the same shall be published in future.

*****End of document*****