Position Paper from the Telecommunications Regulatory Authority of the Kingdom of Bahrain on the Internet of Things

22 February 2023

LAD 0223 010

Introduction

1 The purpose of this position paper (the **"Paper"**) is to clarify and affirm the Telecommunications Regulatory Authority's ("**the Authority**") position in relation to the various policy considerations underpinning the provision of Internet of Things ("**IoT**") services in the Kingdom of Bahrain.

2 This Paper is a position paper only. It is a general statement of the Authority's current views on the provision of IoT services based upon the facts available to it. As advances are made and technological innovation develops in relation to IoT services, the Authority's position may change, and the Authority reserves the right to amend its position accordingly.

3 In this Paper the term "IoT" is used to refer to a global, distributed network (or networks) of physical and/or virtual objects that are capable of sensing or acting on their environment and able to communicate with each other, other machines or computers.[1]

4 In the preparation of this Paper the Authority has taken into account, where appropriate, the approaches being taken in three other jurisdictions (Saudi Arabia, the UAE and the UK).

Background

5 The Authority is keen to support the development of IoT services with a view of the Kingdom of Bahrain being a leading country in the provision and use of IoT services, as well as the deployment of IoT devices. The Authority also wishes to enable IoT services to develop in a coherent, safe and secure manner, whilst promoting innovation and competition.

6 This Paper shall act as an indication to licensees and relevant stakeholders as to the Authority's current viewpoint on a number of policy issues. The Authority, however, reserves its right to amend its position with or without notice.

7 This Paper should not be relied on as an exhaustive statement of the Authority's views on IoT services or the obligations that may apply to providers of such services. Providers must ensure that they comply with all relevant laws applicable in Bahrain, including the

[1] https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf

Legislative Decree No. (48) of 2002 Promulgating the Telecommunications Law (**"the Law"**) and all relevant regulations and other instruments issued by the Authority.

8 Ministries and other regulators may develop their own guidelines or policies relating to IoT services and operators should ensure that they also comply with any such applicable guidelines or policies.

Executive summary

9 This Paper considers the following policy issues in relation to IoT services and a summary of the Authority's position is provided below:

- **Data Privacy:** where the use of IoT services involves the collection and use of personal data and/or sensitive personal data, the Authority considers that such will be regulated by the existing data protection laws and regulations applicable in the Kingdom.

- **Network and Equipment Security and Resilience:** as IoT services develop and consumers become more reliant on them, it will be important that the licensed networks and/or equipment delivering these services are robust and secure. Although IoT services are not explicitly referred to in the current regulations pertaining to network security, the Authority considers that those rules/ regulations apply in relation to such services and that Licensees should have regard to their purview. Further to this, the Authority recommends that where an IoT service requires the use of IoT devices, that those devices be manufactured in accordance the European Telecommunications Standards Institute (ETSI) EN 303 645 standard for the security of IoT devices.

- **Availability of Spectrum:** the Authority recognises the importance of ensuring that sufficient spectrum is available to support and encourage the development of IoT services and will therefore be considering when and where it may be appropriate to license additional spectrum that can be used for such services. Where an IoT service requires the use of spectrum, the provider should either (i) enter into an arrangement with an existing licensee that is entitled to use the relevant spectrum; or (ii) apply for its own frequency licence in relation to the

relevant spectrum[2]; or (iii) utilize "license exempt"[3] frequencies listed in Resolution No. 8 of 2017 Regarding Regulation of Type Approval for Short Range Devices (as may be amended from time to time) (**"the SRD Regulation"**).

- **IoT Identifiers:** Although telephone numbers are not the only identifiers available for IoT devices, the development of IoT services is likely to increase demand for telephone numbers. Prospective providers of IoT services may utilize numbers from the "Universal Number Series" for the purpose of assigning identifiers to their IoT devices. The Authority will also be reviewing the National Numbering Plan and studying the feasibility of introducing a separate number range for IoT devices.

- **Licensing:** where the provision of IoT services triggers one of the three limbs of Article 24(a) of the Law, a licence will be required. Prospective IoT service providers that wish to provide IoT services which involve the operation of a Public Telecommunications Network[4] in Bahrain will therefore need to apply for the most appropriate licence.

- **Type Approval:** the type approval regulations and approvals currently required by the Authority also apply to IoT services and devices. Therefore, as discussed below, importers and distributers should comply with the applicable provisions of these regulations.

- **SIM Card Registration Requirements:** where IoT services require the use of SIM cards issued by local Licensed Operators, generally, prospective IoT providers may only do so following compliance with the provisions of the SIM-Card Enabled Telecommunications Service Registration Regulation[5].

[2] Pursuant to Article 32(a) of the Law, a Service License will be required where it is determined that the frequency license obtained will be used to operate a Public Telecommunications Network.

[3] The phrase "license exempt" is not used in the SRD Regulation. However, use of frequency bands listed in the SRD regulation does not require the user to obtain a Frequency License from the Authority.

[4] As defined in Article 1 of the Law as: "a Telecommunications Network used, in whole or in part, for the provision of Public Telecommunications Services provided either by a Licensed Operator of the Telecommunications Network or a third party."

[5] Resolution No. (13) of 2015 Promulgating the SIM-Card Enabled Telecommunications Services Registration Regulation

- **Embedded SIM Cards[6]:** where an IoT device contains an Embedded SIM Card that requires activation by a local Licensed Operator, prospective IoT service providers must seek the Authority's prior approval to ensure that all SIM-Cards which are used in the provision of IoT Services are configured to be used only for the automated communication between devices and are registered and activated in line with the provisions of the SIM-Card Enabled Telecommunications Services Registration Regulation.

- **Permanent Roaming[7]:** as discussed further below, the Authority has decided that it will, for the time being, permit the permanent roaming of IoT devices provided that the requirements of any local lawful enforcement agency (as may be updated from time to time) are met.

10 The remainder of this Paper discusses these issues in further detail.

IoT and IoT Services

11 Although "IoT" has become a commonly used term, it is difficult to give a precise internationally accepted definition for IoT services, given the wide range of applications that have already emerged and are in the process of being developed. In this Paper the term "IoT Service" is used to refer to a service comprising of a set of functions and/or facilities offered to a user that can be accessed via a smart device, through a voice assistant and/or through other smart user interfaces.

12 IoT Services are commonly associated with machine to machine ("**M2M**") services, which have been defined as services involving an automated transfer of data and information between devices or software-based applications with limited or no human interaction.[8] However, M2M services are now widely regarded as a subset of IoT Services rather than a separate standalone category. For the purposes of this Paper, the Authority therefore uses the term IoT Services to include M2M services.

[6] For the purposes of this Paper, "Embedded SIM (eSIM) shall means a Subscriber Identity Module (SIM) that is physically integrated into the device and cannot be removed or replaced with another SIM."

[7] For example, according to BEREC's report on "Enabling the Internet of Things", the need for permanent roaming may arise where the IoT device is sold outside the country of production but uses a SIM Card with an International Mobile Subscriber Identity (IMSI) of the country of production.

[8] See Recital (249) of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

13 IoT Services have a wide range of uses, such as smart homes, smart cities, tracking, smart metering and connected cars. IoT Services are also increasingly being used in different sectors such as health, agriculture, utilities and transportation.

14 It is important to note at the outset that IoT Services can be provided using wired and wireless networks. They can be classified according to the networks used into:

14.1 IoT Services provided by means of fixed networks;

14.2 IoT Services provided through mobile networks; and

14.3 IoT Services provided through wireless networks using spectrum other than that used by mobile networks, including satellite networks.

15 Across jurisdictions this broad treatment of IoT Services has also been reflected in the differing regulatory approaches to the relevant legal issues.

16 For the purposes of this Paper, the Authority believes that a prescriptive definition of key aspects of IoT being established would be necessary. Therefore, the following terms shall have the meanings ascribed to them below:

16.1 "IoT" means a global, distributed network (or networks) of physical and/or virtual objects that are capable of sensing or acting on their environment and able to communicate with each other, other machines or computers.[9]

16.2 "IoT Service" means a service comprising of a set of functions and/or facilities that users can access via a smart device, through a voice assistant and/or through other smart user interfaces.

16.3 "IoT Service Provider" means any Person[10] that provides an IoT Service to users (including individuals, businesses and the government).

Data Privacy

17 The Authority believes that it will be an important consideration that effective steps are taken to ensure that any consumer data privacy concerns are appropriately addressed as

[9] https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf

[10] As defined in Article 1 of the Law as: "any natural person, juristic entity or public authority."

IoT Services continue to develop. Although it is the case that, for many applications, personal data will not be created or used, there are other applications where it is likely that personal data will inevitably be involved and in some cases it will be a requirement.

18 A potential example would be where an IoT device is used to gather health data about an individual and then transfer that data to a healthcare provider, which then uses the data to provide personalised healthcare services to the individual.

19 Where personal data and/or sensitive personal data is involved, the existing data protection laws in Bahrain will apply.

20 Where the provision of IoT Services entails the processing and transfer of personal data and/or sensitive personal data, IoT Service Providers are required to ensure the compliance with the provisions of Law No. (30) of 2018 with respect to Personal Data Protection (**"the PDPL"**), and more specifically the following obligations therein:

20.1 personal data is processed fairly and lawfully;

20.2 personal data is collected for a specific, explicit and legitimate purpose and shall not be further processed in a way incompatible with the purpose for which it was collected.

20.3 personal data be adequate, relevant and not excessive in relation to the purpose for which it was collected or further processed;

20.4 personal data is correct, accurate and, where relevant, kept up to date; and

20.5 personal data is not kept in a form which permits identification of data subjects once the purpose for which the data was collected or further processed is achieved.

21 Where sensitive personal data is processed, the Authority encourages IoT Service Providers to refer to Article 5 of the PDPL.

22 In the event that the IoT Service Provider intends to transfer personal data outside the Kingdom, it may only do so if[11]:

22.1 The transfer is to a country or territory that is listed in a record compiled and updated by the Personal Data Protection Authority, comprising of countries and

[11] Article 12 of PDPL

territories that, upon the Personal Data Protection Authority's discretion, provide adequate legislative and regulatory protection for personal data[12]; or

22.2 A transfer occurs upon the Personal Data Protection Authority's authorisation on a case-by-case basis provided that the data will be subject to an adequate level of protection.

23 In addition to the PDPL, the Authority is currently proposing to introduce an additional sector specific regulation on the privacy of individuals and data protection in the telecommunications sector, which will be applicable to Licensed Operators in the Kingdom.

Network and Equipment Security and Resilience

24 As IoT Services develop and there are an increasing number of services which users rely on, the Authority believes that it will be important to ensure that the networks and equipment delivering these services are sufficiently robust and secure.

25 The Authority encourages all Suppliers[13] of IoT devices to ensure that all IoT devices imported to the Kingdom are manufactured in accordance with the European Telecommunications Standards Institute (ETSI) EN 303 645 standard[14]. The key requirements of the ETSI standard are that:

25.1 all IoT device passwords are unique per device or user defined;

25.2 the software used in the device is secure and kept up to date. Updates should be provided for the entire lifecycle of the product;

25.3 a vulnerability disclosure policy is provided to enable consumers to disclose vulnerabilities;

[12] The record of countries and territories is listed in Order No. (42) of 2022 Regarding the Transfer of Personal Data outside the Kingdom of Bahrain.

[13] Defined in Article 1 of the Type Approval Regulation as: "anyone who manufactures, imports, distributes, sells or offers for sale Telecommunications Equipment, including the licensed operator importing Telecommunications Equipment for use on its own network."

[14] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

25.4 consumers are provided with clear and transparent information on how and why their personal data is processed, as well as who collects and processes their data (including third parties that could be involved, for example advertisers);

25.5 personal data is secured during transfer and storage; and

25.6 the default settings of the product or service should be set to protect the consumers.

26 The underlying licensed communications provider providing connectivity will be subject to the following regulations concerning network security and resilience:

26.1 Resolution No (9) of 2009 Promulgating a Regulation requiring Licensees to Implement Lawful Access. Under said regulation, the Licensee is required to:

a) Implement lawful access;

b) Retain access related information; and

c) Identify the location of mobile telecommunication services subscribers.

26.2 Resolution No (5) of 2017 Promulgating the Regulation on Critical Telecommunications Infrastructure Risk Management. Wherein every licensee is required to take all appropriate measures to manage risks to the security and availability of its infrastructure and take all appropriate steps to protect, so far as possible, the security and availability of its infrastructure. There are also additional obligations on licensees employing critical telecommunications infrastructure, which includes infrastructure which is essential for the maintenance of health, safety and national security, as well as any centralised system that stores and processes personal data.

27 Although these rules do not refer explicitly to IoT Services, the Authority considers that licensed networks used to deliver IoT Services would be covered by them.

Availability of Spectrum

28 The Authority recognises the importance of ensuring that sufficient spectrum is available to support and encourage the development of IoT Services.

29 In the meantime, where an IoT Service requires the use of spectrum, the IoT Service Provider should either:

29.1 enter into an arrangement with an existing licensee that is entitled to use the relevant spectrum (such as one of the mobile operators); or

29.2 apply for its own frequency licence in relation to the relevant spectrum; or

29.3 utilize short-range radiocommunication devices which operate on "license exempt" frequencies listed under the SRD Regulation provided that:

a) The utilization of the frequencies does not cause harmful interference to licensed and planned services;

b) The user(s) of the frequencies does not claim protection from interference caused by licensed and planned services; and

c) The user(s) of the frequencies must immediately stop the provision of IoT Services if requested by the Authority or any other competent authority in Bahrain.

IoT Identifiers

30 IoT devices usually require an identifier in order to allow them to communicate with other IoT devices.

31 One possibility is for traditional telephone numbers to be used as identifiers, in much the same way as phone numbers are currently used for mobile and other devices. If so, the development of IoT Services is likely to significantly increase the demand for telephone numbers.

32 At present, Licensed Operators may utilize numbers from the "Universal Number Series"[15] for the purposes of assigning IoT identifiers to IoT devices. The Authority is currently studying the feasibility of introducing a dedicated 12-digit numbering range for IoT to the National Numbering Plan.

33 Pursuant to Article 4.3.1.1 of the National Numbering Plan, only holders of individual licenses are eligible to apply for number allocations. IoT Service Provider will therefore only be able to utilize numbers from the National Numbering Plan if they are holders of individual licenses.

[15] As per the National Numbering Plan, Universal Numbers from the 8-digit Universal Number Series 6 and 7 may be used "for any purpose except for Special Services and Premium Rate Services."

Licensing of IoT Services

34 The Authority is responsible for the regulation of the Telecommunications sector in the Kingdom of Bahrain. Telecommunications, as defined in the Law is *"the conveyance and/or routing of messages, sounds, visual images or signals on Telecommunications Networks, other than Broadcasting".* As per the definition in paragraph 16.2 of this Paper, the Authority does not believe that IoT Services are covered by the definition of telecommunications and that therefore a telecommunications licence is not required to provide an IoT Service. However, the means by which IoT Services are provided, namely Telecommunications Networks are within the Authority's purview and as such may require a licence for their operation.

35 Pursuant to Article 24(a) of the Law, *"no Person shall operate a Public Telecommunications Network, any Telecommunications Network using a Telecommunications Frequency or provide a Telecommunications service in the Kingdom except after obtaining a License for that purpose in accordance with the provisions of the Law".*

36 Article 24(a) of the Law is therefore the starting point for licensing considerations vis-à-vis the provision of IoT Services. Article 24(a) of the Law sets out three criteria which trigger a licensing requirement:

36.1 the operation of a Public Telecommunications Network;

36.2 the operation of a network that uses a Telecommunications Frequency; or

36.3 the provision of a Telecommunications service

37 The Authority finds it necessary to clarify that although the second limb of Article 24(a) of the Law does not differentiate between the operation of a "public" or "private" Telecommunications network, the licensing implications in place for the two types of networks would differ. Where a Person[16] operates a Public Telecommunications Network that uses a Telecommunications Frequency, both, a Frequency License and Telecommunications License would be required. Whereas the operation of a private Telecommunications Network (which for the purposes of this Paper has been defined as a Telecommunications Network providing connectivity which would only benefit one

[16] Any natural person, juristic entity or public authority.

person, or a group of persons who have common ownership and is not made available to the public and not provided for remuneration) that uses a Telecommunications Frequency may necessitate a Frequency License only.

38 Prospective IoT Service Providers operating a private Telecommunications Network would not be required to obtain a Telecommunications License. However, a Frequency License may be required as may be determined by the Authority on a case-by-case basis.

39 Prospective IoT Service Providers who wish to provide IoT Services utilizing the connectivity provided by one of the existing Public Telecommunications Networks in the Kingdom may do so without the need to acquire a license under Article 24(a) of the Law.

Type approval

40 The Authority's review of the regimes for type approvals for IoT devices has shown that in the majority of cases, the existing type approval regimes have merely been applied to IoT devices.

41 The Authority therefore confirms that its current type approval regulations in force will likewise apply to IoT devices. The relevant regulations are:

41.1 the Authority's Resolution No. (9) of 2017 promulgating the Regulation on the Type Approval and Importation of Telecommunications Equipment connected to Public Telecommunications Networks (the "Type Approval Regulation"), the objective of which is to regulate the approval and importation of Telecommunications Equipment that is part of or connected, or comprises, a Public Telecommunications Network; and

41.2 the SRD Regulation, the objective of which is to regulate the approval, importation and use of short range devices.

42 The salient obligations under the Type Approval Regulation are that all Telecommunications Equipment manufactured, supplied, imported, distributed, sold, offered for sale or connected to a Public Telecommunications Network meet the technical requirements listed in paragraph 85 of this Paper and are issued with a Type Approval Certificate from the Authority.

43 IoT device Suppliers must ensure that the Telecommunications Equipment meet the technical requirements stipulated under the Type Approval Regulation:

43.1 It does not use easily accessible software interface or simple physical modification, be capable of being configured to operate on radio frequency, which are not designated for public telecommunications purposes in the Kingdom.

43.2 It shall not cause any harm to the user, general public or staff working on Telecommunications Networks.

43.3 It shall not generate electromagnetic disturbance exceeding the level above which Telecommunications Equipment or other equipment cannot operate as intended.

43.4 It shall have a level of immunity to the electromagnetic disturbance expected in its intended use which allows it to operate without unacceptable degradation of its intended use.

43.5 It shall efficiently and effectively use the radio spectrum allocated so as to avoid harmful interference.

43.6 It shall not cause any damage to Telecommunications Networks or interfere with the correct working of a Telecommunications Network or misuse network resources, thereby causing an unacceptable degradation of services.

43.7 It must be interoperable with other apparatus and be connected to interfaces of the appropriate type in the Kingdom.

43.8 Where it is a terminal device, it shall meet the following additional conditions:

a) If it is a mobile terminal device, it must have an IMEI number;

b) It shall support certain features to safeguard the personal data and the privacy of Users and Subscribers;

c) It shall support certain features of ensuring avoidance of fraud;

d) It shall support special features ensuring access to emergency services; and

e) It shall support certain features in order to facilitate its use by Users with a disability.

44 Notwithstanding the above, IoT devices intended for private use may be imported into the Kingdom without the need to acquire a Type Approval Certificate if any of the following conditions (listed under Article 6(c) of the Type Approval Regulation) are met:

44.1 CE Marked Telecommunications Equipment without radiocommunications interfaces;

44.2 CE Marked Telecommunications Equipment or other CE Marked devices or apparatus supporting one or more of the following interfaces:

a) Terminal Devices, such as DECT, GSM, UMTS, LTE and others within the approved frequencies and permitted for such applications.

b) Bluetooth if incorporated within Telecommunications Equipment.

c) Wireless LAN (IEEE802.11 series of standards)

d) Equipment with CE Mark for reception only.

e) Passive Telecommunications Equipment and ancillary equipment, devices and apparatus, including information technology equipment and connection and power cables.

45 Where IoT device Suppliers wish to import and use short range devices, they may only do so following compliance with the technical requirements listed in Annex 1 to the SRD Regulation[17] and following the issuance of a Type Approval Certificate from the Authority.

46 IoT device Suppliers[18] should therefore comply with any applicable provisions of these regulations and all future regulations, determinations and requirements issued by the Authority or other authorities in Bahrain concerning the approval and importation of Telecommunications Equipment[19] and short range devices.

SIM Card Registration Requirements

[17] https://www.iga.gov.bh/Media/Publications/pdf/The%20Regulations%20of%20Type%20Approval%20for%20Short%20Range%20Devices.pdf

[18] Type Approval Regulation (n 34).

[19] Defined in the Telecommunications Law as: "any equipment or apparatus used or intended to be used for Telecommunications and that is part of or connected to, or comprises, a Telecommunications Network, and includes Radiocommunications Equipment."

47 The Authority's position is that where an IoT Service Provider requires the use of SIM cards issued by a local Licensed Operator, generally it may only use the SIM cards following compliance with the provisions of the SIM-Card Enabled Telecommunications Services Registration[20]

48 Where an IoT device contains an Embedded SIM Card that requires activation by a local Licensed Operator, it must seek the Authority's prior approval to ensure that all SIM-Cards which are used in the provision of IoT Services are configured to be used only for the automated communication between devices and are registered and activated in line with the provisions of the SIM-Card Enabled Telecommunications Services Registration Regulation.

Permanent Roaming

49 Roaming is a well-established principle in the sphere of mobile voice telephony, allowing individuals to "roam" on mobile networks in other countries when they are travelling outside their home country.

50 Roaming could also arise in relation to IoT devices and services, for example where an IoT device is imported into Bahrain and makes use of a SIM card which is issued by a mobile operator not licensed by the Authority. The IoT device may remain in Bahrain indefinitely, giving rise to the potential need for permanent roaming arrangements, if the IoT device is to continue to function in Bahrain.

51 The Authority believes that permanent roaming is in principle permissible provided that:

51.1 the requirements of any local lawful enforcement agency (as may be determined on a case-by-case basis) are met; and

51.2 the SIM cards used in the provision of the IoT Service are configured to be used only for automated communication between devices.

52 This means that permanent roaming is not prohibited but will be monitored from time to time. In this context, it will be important to keep under review any associated security issues, in light of the risk of foreign IoT devices being used for malicious purposes.

[20] The SIM-Card Enabled Telecommunications Services Registration Regulation dated 7 January 2016.

Conclusion

53 As noted above, the Authority may issue in the future a regulation or guidelines in relation to IoT Services. Until such time, this Paper sets out the Authority's views on the relevant policy issues relevant to IoT and IoT Services. Persons who are unsure of their obligations concerning the provision of IoT Services should reach out to the Authority and seek clarification.