Telstra Wireless Application Development Guidelines

Version 13 Issue 1

Date: January 2024

TABLE OF CONTENTS

1. AIM

The goal of this document is to inform developers of solutions to utilise cellular connectivity on Telstra's mobile network more effectively:

1. Consider the key factors for the user requirements e.g. long battery life and optimise solutions to meet these requirements; and
2. Encourage efficient use of the Telstra mobile network by developers, to enhance customers' experience of the Telstra mobile network.

It is important that solution developers understand how to develop for Telstra's mobile network. Your design choices can have significant effects on how well your solution works, enhancing the competitive advantage of your product or solution, as well as improving solution performance, via its feature set, longevity and compliance to industry standards.

2. SCOPE

These guidelines cover application development for all cellular connected devices, including M2M and IoT .

M2M and IoT solutions include embedded modules, devices integrating embedded modules and the related controlling software behaviour.

For those requiring additional detail on each topic, links are provided to explore further.

This document excludes details of how to code applications and associated backend servers / cloud, nor does it address details of user interface visual design or programming languages.

This document draws from a wealth of existing industry associations, OS platform, wireless operator and other developer guidelines.

3. DISCLAIMER

These guidelines are general in nature and apply to the most common use-case scenarios.

You should consider your own specific requirements where necessary.

Reliance upon any representations or recommendations made or information contained in this document is at your own risk.

Telstra will seek to update this document periodically. Please check the Telstra.com website for an updated version. If you are building solutions specifically for Telstra or other customers, seek guidance to ensure your solution delivers the product's desired performance.

4. INTRODUCTION

4.1. Why are the guidelines required?

4.1.1. Cellular Network Constraints

Cellular networks have a few factors that developers need to consider when developing their applications such as:

- Power Source: Cellular devices typically rely on batteries whereas home/fixed network routers are AC powered.
- Reliability/Robustness of network connection: Cellular networks provide variable performance, such as throughput and connectivity as radio conditions are constantly changing.
- Network Technology Speed and Latency Variability: Cellular throughputs can vary considerably based on location, terrain, coverage, radio interference, geography and technology.
- Capacity constraints: Applications must be designed to accommodate changing throughput, connectivity and latency when networks are heavily loaded.
- Cellular network evolution: as cellular technologies age, they will not be upgraded as frequently as the focus of development moves to the most current network generation deployed. Developers should utilise the latest generation technology to access the most current feature capabilities which will also provide the greatest device longevity.

4.2. Benefits of the guidelines?

Following the principles in these guidelines will provide benefits for the developer, application/solution user and the network operator. Such benefits can include:

- improved battery life for devices;
- lower data costs – if an application uses the network efficiently, it should result in lower data consumption, resulting in lower data costs for the app user in connection with that application;
- more responsive products;
- increased application / device longevity;
- more robust / resilient applications;
- reduced network signalling; and
- improved user security and privacy.

Section 7 (Application Development Techniques) sets out the techniques which developers can use to deliver the above benefits.

5. AN OVERVIEW OF THE TELSTRA NETWORK

5.1. Technologies and Features

Mobile networks evolve rapidly. Developers need to ensure they future proof their design in such a way to take advantage of new features as they become available.

The following table presents the technologies and features available on the Telstra Network (as of January 2024) along with future technology trends. Included alongside are relevant considerations for designing your wireless application.

Technology/Feature	Present	Future	Considerations
3G Frequency Bands Uses HSPA and HSPA+ technologies	• 850 MHz (B5)	• Telstra will be switching off 3G in June 2024.	• Telstra will be switching off 3G in June 2024. Telstra will not certify any 3G only devices.
4G Frequency Bands Uses LTE technology	• 700 MHz (B28) for coverage • 1800 MHz (B3) for coverage • 2100 MHz (B1) for capacity • 2600 MHz (B7) for capacity and in-building coverage		• Note that the 700 MHz bands (B12, 13, 14, 17) used in the US are not compatible with the Australian 700 MHz band (B28) • Lower frequency bands generally provide better coverage in rural areas.
LTE Carrier Aggregation (CA) Combines 2 or more carriers together to allow greater throughput	Support 2, 3, 4 and 5 CA combinations of bands 1, 3, 3, 7, 7 and 28	No new CA combinations are planned.	• CA offers higher data rates that are suitable for large file downloads and video streaming applications CA is limited to certain areas of the network
5G Frequency Bands	• 850MHz (n26) ** • 2600MHz (n7) • 3.6GHz (n78) • 26GHz (n258)	• 700MHz (n28) ** • 850MHz (n26) • 1800MHz (n3) • 2100MHz (n1) • 2100MHz (n256)	
4G+5G Non-StandAlone (NSA) carrier aggregation	LTE bands + n26A-n78A		Aggregating a low 5G band (n26) with a mid-band (n78) will improve 5G coverage experienced by the user.

Technology/Feature	Present	Future	Considerations
5G StandAlone (SA)	Launched	Will utilise the available launched NR bands	StandAlone networks will facilitate new services to be offered including services requiring very low latency or very high reliability where applicable.
MIMO Multiple In Multiple Out. Using multiple antennas for the up and downlink of radio transmission can increase throughput or received signal quality	In downlink network supports: • 2x2 on all bands • 4x2 on B1, B3, B7 and B28 • 4x4 on B1, B3, B7 and n78 MIMO notation: n x m, n indicates number of antennas at cell, M in the device		
LTE-M/NB-IoT Low throughput and low power cellular technology for IoT solutions	• 700 MHz (B28) for LTE-M and NB-IoT	• 1800 MHz (B3) may be considered for LTE-M	
IPv6 The most recent version of the internet addressing protocol. It has a far larger number of unique addresses than IPv4	• All devices shall support IPv4,IPv6, IPv4v6 however: • Configuration is dependent on many considerations (refer last column) and therefore discuss your device configuration with Telstra Products at time of ranging	• As per present Devices shall support IPv4, IPv6 and IPv4v6. • All applications shall be designed to support IPv6 SS (single stack) natively • Wherever possible # device shall be configured as IPv6 SS for domestic use (non roaming case)	• APNIC no longer has any IPv4 addresses and the industry is moving to IPv6 • Telstra's IPv4 address pools are finite • Consider IP protocol capability of the following: M2M/IOT server, M2M/IOT application, device capability, access technology, service subscription (confirm with Telstra), recommended APN supports (confirm with Telstra) • Whether device supports 464XLAT CLAT and whether network supports PLAT on the chosen APN • Whether the device even requires IP protocol

* Telstra mobile broadband coverage footprint: https://www.telstra.com.au/coverage-networks/our-coverage and Telstra IoT coverage footprint:

https://www.telstra.com.au/business-enterprise/about-enterprise/our-network/iot-coverage-map

This is dependent on APN used and capabilities of any service platforms used. See section 7.5 for more details.

** In July 2024 Telstra will have access to more spectrum in the extended 850MHz band. To date Telstra's 850MHz band was classified as band 5, with the new holdings all of Telstra's existing and new 850MHz spectrum is covered by the band numbered 26. New devices on the Telstra network should support band 26 instead of band 5 to access the full supported band. Band 5 can be considered a subset of band 26. Existing devices declaring band 5 will continue to be supported without change in performance.

5.2. Device Category Network Support

For LTE, "Device categories" refer to different maximum theoretical data rates supported by devices. Devices will have a maximum category that they can support. This needs to be matched by cellular network support to achieve the same maximum category and the possible maximum category assigned is also dependant on network radio conditions.

The following table lists the most common LTE categories supported by the Telstra Network. This is not an exhaustive list. If your device supports a category not specifically mentioned in this table, please contact Telstra so we can help you determine if that device category is supported on our network.

Categories M1, NB1 and NB2 have been designed specifically for IoT (refer to section 0). A key difference between these and traditional LTE categories is that the capability set has been modified to enable lower power consumption, reduced device complexity and lower cost.

A summary of the key LTE categories supported on the Telstra network:

Category	Downlink (max)	Uplink (max)	3GPP Release*
NB1	25.5 kbps	62.5 kbps	Rel. 13
NB2	127 kbps	158.5 kbps	Rel. 14
M1	588 kbps ***	1119 kbps***	Rel. 14
1	10 Mbps	5 Mbps	Rel. 8
3	100 Mbps	50 Mbps	Rel. 8
4	150 Mbps	50 Mbps	Rel. 8
6	300 Mbps	50 Mbps	Rel. 10
9	450 Mbps	50 Mbps	Rel. 11
11	600 Mbps	50 Mbps	Rel. 11
13	390 Mbps	N/A**	Rel. 12
15	800 Mbps		Rel. 12
16	1050 Mbps	N/A**	Rel. 12
13	N/A**	150Mbps	Rel. 12
18	1200 Mbps	N/A**	Rel. 13
19	1650 Mbps	N/A**	Rel. 13
20	2 Gbps	N/A**	Rel. 14
21	1400 Mbps	N/A**	Rel. 14

In the previous table, the downlink and uplink throughputs are theoretical maximums and not indicative of typical user throughputs in a live environment, they are included to allow some comparison between the different categories.

* 3GPP release refers to the release version of industry standard covering the device category.

** Note that as of 3GPP Release 12 the uplink and downlink category speeds have been split so that they can be paired in different combinations. This means that an area which supports a particular category's downlink speed doesn't necessarily support the same category uplink speed. Therefore, UL speed is dependent on the UL category and is independent of the DL category.

*** Maximum speeds achieved with radio device operating in half duplex mode.

5.3. 5G NR RedCap (Reduced Capability)

As part of the standardisation activities for 5G New Radio (NR), the 3GPP standardisation body introduced the ability for networks to support 5G NR devices with reduced capability, aka RedCap. RedCap fills a gap between the low throughputs of the 5G mMTC technologies LTE-M and NB-IoT and the higher throughputs of 5G Mobile broadband. By removing key functionality, a RedCap device is expected to cost less than 5G NR mobile broadband devices. Functionality changes can include:

- Reduction in maximum device bandwidth
- Reduction in the minimum number of receive branches
- Reduction in the number of downlink MIMO layers
- Reduction in the maximum downlink modulation order
- Introduction of half duplex operation

By being less capable than 5G NR mobile broadband devices, the use cases for which RedCap devices may be used, is also reduced. That is, RedCap devices are not intended for applications requiring high throughput like routers and smartphones but may be sufficient for use in wearables, industrial wireless sensors and voice centric devices.

The reduced capability of RedCap devices also places greater demands on the network because RedCap devices don't use network resources as efficiently as regular 5G NR mobile broadband devices.

Despite this increased demand on the network, Telstra intends to support RedCap devices to some degree. Developers may find that requirements are placed on the amount of functionality that can be removed for Telstra Device Certification and are advised to check with their Telstra representative before making a long-term product decision.

RedCap permits some optional features such as 256QAM and 2 receive antennas, for improved device performance it is strongly recommended that these features are supported on the device.

5.4. Internet of Things (IoT)

5.4.1. Introduction

The Internet of Things is an emerging technology trend based heavily on the M2M (Machine to Machine communication) market. IoT systems typically comprise of many (typically hundreds and even thousands) low cost and low power devices which communicate with other devices, microservices and user applications across networks via cloud servers. These devices tend to serve a single function that requires lower data transfer rates and data usage.

For this reason, new device categories were created to address IoT. These new categories focus on addressing the previously unmet needs of these IoT solutions by providing lower throughputs, requiring less energy consumption and extending the effective coverage area of cellular networks.

Telstra recommends developers use these recognised 5G massive machine type communications (mMTC) technology for their IoT solutions. Telstra supports the 5G IoT specific device categories (Cat M1, Cat NB1 and Cat NB2).

5.4.2. 3GPP Power Saving Mode (PSM)

Power Saving Mode is a feature designed for IoT devices to assist in the conservation of battery power with the potential to achieve a 10 year battery life.

While it has always been possible for a device to turn its radio module off to conserve battery power, the device would subsequently have to reattach to the network when the radio module was turned back on, the reattach procedure consumes a small but finite amount of energy. The cumulative energy consumption of reattaches can become significant over the life of a device.

When a device initiates PSM with the network, the device negotiates with the network how long the PSM period will be and the network retains state information and a reattach procedure is not required, even if the device awakes and sends data before the expiration of the time interval it agreed with the network.

As an example, for a monitoring application, the device might be configured by an application to enable PSM, negotiate a 24 hour time interval with the network and provide a daily status update to a centralised monitoring point. If the device's monitoring application were to detect an alarm condition, irrespective of any agreed sleep interval, the application could wake the radio module instantly and send vital information without the need for a full reattach procedure.

In a similar manner to a radio module that has been powered off, a radio module with PSM enabled cannot be contacted by the network whilst it is asleep. The inability to be contacted whilst asleep may preclude the use of PSM for some applications.

5.4.3. 3GPP Extended Discontinuous Reception (eDRX)

Extended Discontinuous Reception is an extension of an existing feature which can be used by IoT devices to reduce power consumption.

Today, many smartphones use discontinuous reception (DRX) to extend battery life. By switching off the receive section of the radio module for a fraction of a second, the smartphone is able to save power. The phone cannot be contacted by the network while it is not listening

but if the period of time is kept brief, the phone user will not experience degradation of service. E.g. If called, the phone might ring a fraction of a second later than if DRX was not supported.

eDRX allows the time interval during which a device is not listening to the network to be greatly extended. For an IoT application it might be acceptable for the device to not be reachable for a few seconds or longer. Whilst not providing the same levels of power reduction as PSM, for some applications eDRX may provide a mechanism to deliver device reachability and reduce power consumption.

5.4.4. 3GPP Coverage Enhancement

Some IoT applications require devices to be positioned in very poor radio conditions where the signal is extremely weak. For example, underground parking garages and in ground pits. The Coverage Enhancement feature has the potential to increase the depth of radio coverage to enable IoT devices to be placed and operate in locations that would otherwise not be possible.

The Coverage Enhancement feature increases the power levels of signalling channels together with the ability to repeat transmissions. Through repeated transmission, the ability of receivers to correctly resolve the message sent is improved. The trade-off is that repeating signal transmissions consumes additional power and the time between battery recharge or replacement may be reduced.

5.4.5. IoT Typical Usage by Device Category

The following table is intended to help developers determine the most suitable device category for their IoT solution. You should choose a suitable device from the most appropriate device category to support the characteristics of your specific application.

Device Category	> = 13	> = 1	1, M1	1, M1, NB1, NB2	M1, NB1, NB2
Device Data Usage (UL+DL bytes per day)	> 10 MB	> 1 MB	0.1 – 1 MB	< 0.1 MB (100 kB)	< 0.01 MB (10 kB)
LTE Bands Required	Triband (B28, B3, B7)	Dual Band (B28, B3)	Dual Band (B28, B3)	Dual Band (B28, B3)	Single Band (B28)
Typical Use Cases	• Video streaming • Connected Car	• Connected Home • Wearables	• Logistics • Remote Healthcare	• Smart City • Energy Metering	• Environmental Monitoring • Industrial Sensors

5.4.6. Telstra IoT Connection Management

Telstra offers connection management platforms which allow IoT/M2M business customers to easily manage their IoT/M2M deployments. These are cloud services with a web based dashboard interface, which provide users with a single access point from where they can:

- Activate and deactivate SIMs/services;
- Run near real-time diagnostics and get diagnostic alerts;
- Review connection session history and near real-time connectivity status;
- Control data usage costs;
- Set business rules and customised alerts to identify abnormal activity or device failures;
- Run customised reports to get service and usage statistics; and
- Use an API to interface with external server applications to automate tasks.

IoT Connection Management platforms may have a location service feature, which provides a capability to monitor the location of devices. This feature does not require the device to support GPS and instead makes use of the Telstra cellular network. It can act as a backup service in case of GPS failure to locate and detect movement of devices across cell towers.

More information on Telstra's Connection Management Platforms can be found at:

https://www.telstra.com.au/business-enterprise/products/internet-of-things/capabilities/connection-management-platform

5.4.7. Telstra IoT Platform

The Telstra IoT Platform is a cloud based service with device management, data collection, visualisation and analytics capabilities. The IoT Platform paired with Telstra certified devices and Telstra mobile network connectivity services can be used to build an end to end IoT solution. The IoT Platform provides users with the ability to:

- Manage device configurations, settings and software/firmware updates over the air;
- Manage and store incoming data streams from client applications on deployed devices/sensors;
- Analyse and visualise data to generate actionable insights and business intelligence; and
- Integrate Platform services with external applications/microservices using RESTful APIs.

More information on the Telstra IoT Platform can be found at:

https://www.telstra.com.au/business-enterprise/products/internet-of-things/capabilities/cumulocity

The Telstra IoT Platform is built on top of Cumulocity IoT. The guides listed below provide the steps a developer can use to integrate their IoT systems with the Cumulocity platform. Developers should consider using modules with native support for LWM2M or MQTT protocol stacks to simplify device integration with the IoT Platform.

- General guide on Cumulocity's RESTful API: https://cumulocity.com/api/
- Guide on developing device client applications for interfacing with Cumulocity (Eg using MQTT): https://cumulocity.com/guides/device-integration
- Guide on developing external microservices/server applications for interfacing with Cumulocity: https://cumulocity.com/guides/microservice-sdk/introduction/

5.5. Telstra Network Technology Closure

The Telstra 2G network was shut down on the 1st of December 2016. Existing 2G-only products (handsets, IoT/M2M applications, etc.) ceased to have mobile connectivity from this date.

Telstra will be switching off 3G in mid-2024. After that network closure, you will still be able to access the Telstra Mobile Network provided your device is 4G or 5G compatible and supports Telstra's frequency bands. If voice support is required then VoLTE will need to be supported.

For our customers in a 3G only coverage area, we plan to establish 4G coverage in all 3G only areas by the time of 3G closure. The new 4G coverage will be similar in size and reach as pre-existing 3G coverage.

For further information, please refer to https://www.telstra.com.au/support/mobiles-devices/3g-closure

To provide IoT/M2M devices with the longest possible support, Telstra recommends using the most recent technology available. Telstra considers the 5G mMTC technologies of NB-IoT and LTE-M as the preferred choice for IoT /M2M applications because they:

- Have a longer life expectancy;
- Can support more devices per unit area; and
- Supports new IoT/M2M specific device categories (see section 0) with better power consumption, lower cost and better coverage characteristics

Whilst Telstra has not yet committed to any closure date for our 4G LTE network, at some point it will eventually be closed down. As the recognised technologies for 5G mMTC, Telstra anticipates support for both NB-IoT and LTE-M to be maintained after the closure of our 4G network. This may mean that devices based on these technologies may be a better choice for M2M/IoT applications as other device categories like Cat 1 or Cat 4 will cease to operate after our 4G LTE network closes.

5.6. Telstra Certified Devices

Telstra believes in customer first and puts the customer at the centre of everything we do. The Telstra certification and testing program is designed to ensure that your device is compatible with our network.

Telstra recommends only devices or modules certified by Telstra be used on our network.

Telstra certification will help ensure devices are able to inter-operate with Telstra's network by validating areas such as:

- Frequency band support;
- Data throughput performance across all networks including 3G, 4G, 5G and Wi-Fi if applicable;
- device behaviour in stationary and mobile conditions;
- Device performance under congested network environments;
- Network reacquisition and retry algorithms;
- Data and device stability;
- Radio compliance;
- Antenna sensitivity;
- Over the air firmware and application upgrades;
- IPv6 functionality; and
- Battery life for low power devices.

The following guidelines outline the process to have your device tested and approved by the Telstra M2M Device Certification Program: https://www.telstra.com.au/content/dam/tcom/business-enterprise/machine-to-machine/pdf/business-enterprise-m2m-device-certification.pdf

Telstra recommends integrating a certified module in your end use/finished device, which will significantly expedite the testing process. A list of Telstra certified IoT/M2M modules and devices can be found at: https://www.telstra.com.au/content/dam/shared-component-assets/tecom/iot/capabilities/certified-devices/telstra-m2m-certified-devices-modules.pdf

Please check that you have the latest approved Telstra module list, as this is updated frequently.

6. CONSIDERATIONS FOR DEVICES INTEGRATING MODULES

6.1. Appropriate Technology Choices

6.1.1. Description

When selecting an embedded module for an integrated IoT/M2M device, a developer should consider the module's supported cellular features and capabilities for the proposed application.

6.1.2. Methods

6.1.2.1. Appropriate Cellular Technology Choice

LTE only modules are available as well as multimode LTE + 3G modules. Some newer modules also support 5G. With our 3G closure scheduled in mid-2024, Telstra will no longer certify 3G only solutions.

6.1.2.2. Coverage / Radio Network Technology Support / Frequency Band Support

It is important to ensure that LTE and/or NR coverage is available over the entirety of the expected usage areas. Telstra's coverage is constantly expanding so developers should refer to our coverage maps for the latest information at: https://www.telstra.com.au/coverage-networks/our-coverage or https://www.telstra.com.au/business-enterprise/about-enterprise/our-network/iot-coverage-map

Refer to the table in section 5.1 of this document for information regarding Telstra's current and future frequency band support for 3G, 4G and 5G technologies.

6.1.2.3. Throughput performance

Choose a module based on your IoT/M2M solution's throughput and data usage requirements. See table in section 5.4.5 for guidance on choosing the appropriate device category based on typical IoT use cases.

As a general rule, the higher the data throughput required, the faster device category should be selected. This will reduce the time connected to the network, which is the highest device power consuming state and improves end user experience.

6.1.2.4. Choose devices /modules certified for use on Telstra's network

Certified modules have been tested by Telstra for compatibility with Telstra's network.

Approved modules and devices will typically have better longevity due to greater compatibility with our networks - features, technology and frequency bands.

For non-approved modules and any devices integrating them, there can be no guarantee that they will work with our network currently or into the future.

For IoT/M2M integrated device approval, there is a streamlined process for devices integrating previously approved modules

6.1.2.5. Data only or Voice and Data

Note when selecting an embedded module - some modules only support data and others support both voice and data. If the application doesn't require voice, then a data only module is recommended as it is likely to be cheaper and less complex.

6.1.2.6. FOTA (Firmware over the air)

FOTA is a requirement for all cellular capable modules and devices to be certified for use on our network.

Having the ability to address bugs and update devices remotely saves customers time and energy down the track. This is especially true for an IoT solution that may feature hundreds or even thousands of deployed devices as it would not be practical to physically attend to each device individually to install a software patch or update.

6.1.2.7. Module Radio Network Features

Choose modules that support important radio network features such as:

- CDRX (Connected mode Discontinuous Reception) – this is a device feature that allows the device to have micro sleeps. This feature allows the device to reduce battery consumption while minimising impact to latency.
- eDRX (extended Discontinuous Reception) – this is an IoT device feature that requires network support. It allows the time interval during which a device is not listening to the network to be greatly extended, reducing battery consumption.
- PSM (Power Save Mode) – this is an IoT device feature that requires network support. The device will inform the network that it will be going into power save mode (using close to no power in this state) along with information about when it will 'wake up' for a short period to receive any messages that may be waiting.
- RAI (Release Assistance Indicator) – this is an IoT device feature that requires network support. It allows the device to indicate to the network that it is not expecting to receive/transmit any more uplink/downlink data. Upon receiving this signal the network moves the device into an idle state immediately rather than relying on an inactivity timer to expire, reducing battery consumption.

6.2. Regulatory Considerations

When integrating a module into a device, regulatory requirements need to be met.

These are captured by the ACMA RCM - Regulatory Compliance Mark for the product (and embedded module).

The RCM indicates a device's compliance with applicable ACMA technical standards – that is, for telecommunications, radio communications, EMC and EME.

Refer: https://www.acma.gov.au/step-5-label-your-product

6.3. Antennas

The antenna is one of the most critical components of a device and often the component that is given the least amount of thought. There are lots of antennas advertised for sale which might work well in overseas markets. These antennas may be relatively inexpensive because of their extensive use in other countries and therefore might be perceived as a way to reduce device cost. However, due to the different frequencies in use in Australia, these antennas may provide poor performance. A consequence of which, devices using these antennas may not achieve the coverage expected, leaving end users disappointed.

- The 3GPP mobile radio standards define how many antennas each device category shall support and devices shall comply to these requirements. Reducing the number of antennas has a negative impact on the received signal which impacts performance and customer experience.
- Antennas should support all frequencies bands supported by both the module and network.
- Antennas should be optimised to suit the frequency bands to be used by the device.
- For 3G devices they should be optimised for band 5 (850 MHz).
- For 4G devices they should be optimised for all the bands they support and especially bands 3 (1800 MHz) & 28 (700MHz)
- For 5G devices they should be optimised for all the bands they support and particularly bands n78 (3.6 GHz), n7 (2.6 GHz), n258 (26 GHz) and n26(850 MHz).
- When installing remote equipment, directional antennas should (in most cases) be oriented toward the strongest received signal.
- Within the physical constraints of the end product, antennas should be configured and placed to optimise radio performance. Mounting location and space allocation should be considered in the early phases of the product development process to maximise performance.
- Pattern shape is another antenna performance parameter that should not be overlooked. An omni directional type pattern is much more desirable than the directional one. Parasitic coupling to metal structures near the antenna can alter its pattern shape and operational bandwidth.
- To minimise interference, it is recommended that the positions of the antennas are as far as possible from any digital circuitry that generates high frequency noise (e.g. high speed clocks).
- Telstra recommends where a radio device category supports multiple antennas to support MIMO or receive diversity, then those multiple antennas be used. For example, 2 antennas for Cat 1 and 4 antennas on Cat 16 and above.

6.4. RF Shielding / Interference Mitigation

Integration of wireless modules into end products shall minimise any possible interference with other components.

6.4.1. Radio Interference with Device Components:

- Radio interference in the end device is typically sourced from circuits such as CPU, memory chips, video circuits and other components generating high frequency

electrical noise which has the potential to couple into the radio through the antenna or other conducted paths. Such interference affects the overall wireless performance and user experience. For example, the screen resolution used by a PC or laptop operating nearby may interfere with cellular radio signals and impact the user experience.

- The Embedded Device design should consider the integration of a radio module and minimise interference between the host system components and the embedded module and associated antenna subsystem.

6.4.2. Coexistence with other wireless technologies

- Attention needs to be paid to coexistence with other wireless technologies likely to be resident in the same unit. There should also be no interference between the cellular radio interface and other radio interfaces present in the product (e.g. WiFi).

6.5. Device Identification

The IMEI ranges of the wireless modules embedded into the end product must be submitted to Telstra on a regular basis (for Telstra Certified Devices). Submission details are provided upon initiating certification process.

- IMEI – International Mobile Station Equipment Identity – is a unique identity code used by network operators to distinguish between devices on our network.
- TAC (Type Allocation Code) refers to the first eight digits of the 15 digit IMEI code and identifies the manufacturer and model of a device.

Telstra prefers that devices integrating modules to have a different TAC code to the embedded module - this allows easier management of the device group on the network. If this is not done then Telstra prefers a separate IMEI series within the TAC range to allow devices to be readily identified. It is strongly recommended to update the SVN (software version number) with each new release to make it easier to track which devices have moved to the latest module firmware update.

6.6. eSIM

An embedded SIM (eSIM) is a hardware secure element which holds the subscription profile of a mobile network operator that can be embedded/soldered into a device.

eSIMs are reprogrammable, enabling remote provisioning and management of services over the air.

eSIMs are supported by the Telstra Network. Contact Telstra by email at TelstraWirelessM2MHardware@team.telstra.com to discuss deployment and use of eSIMs in your device.

6.7. Ruggedness

- Ensure devices are appropriately hardened / ruggedised against the elements for remote field deployment where relevant.
- Ensure devices have sufficient protection to prevent theft of UICC (SIM). Devices should have a sealable, tamper proof enclosure.

7. APPLICATION DEVELOPMENT TECHNIQUES

7.1. Best Practices for Development

When developing applications, Telstra recommended best practise would consider the following points:

- Have interoperability / compatibility with the Telstra Network
- Minimise unnecessary data transfers
- Optimise any necessary data transfers
- Minimise unnecessary signalling overhead
- Be resilient to changing network conditions
- Be responsive
- Be secure
- Comply with industry and regulatory requirements
- Be serviceable
- Be lifecycle managed
- Conserve power

A series of techniques referencing industry standards and guidelines that can assist developers in implementing best practices outlined above are described in the following sections.

7.2. Fundamental Methods

7.2.1. Description

The GSMA Developer Guidelines (https://www.gsma.com/iot/iot-device-application-developers/) outline several techniques to optimise the performance of smart phone applications with mobile connectivity. These techniques are equally applicable to IoT/M2M applications.

The guidelines recommend use of the methods listed below for developing the ideal mobile application, addressing many of the best practices listed in Section 7.1.

7.2.2. Methods

7.2.2.1. Asynchrony

To maximise user satisfaction, applications should be designed to be responsive which can be achieved using asynchronous logic for the main code block.

- Make use of separate parallel threads for independent network requests
- The main application thread handling the user interface should not be blocked by outstanding responses to network requests.
- Progressively load and present network response/data as it arrives to the user. Do not wait for all responses to return successfully before providing an update to the user.

7.2.2.2. Connection Loss and Error Handling

- Request types: Categorise network requests as user initiated (primary), non-user/system initiated and secondary (spawning from primary requests) to determine appropriate actions in event of network issues.
- Cancellation: Allow users the ability to cancel primary requests. Cancellation of primary requests should result in cancellation of secondary requests.
- Error handling: Make use of notifications upon failure of primary requests. After attempting some limited number of retries, suspend the request and present the option to resume the request manually. See Section 7.3 for guidance on appropriate use of retry mechanisms.
- Download resumption: Divide large download files into chunks to make use of download resumption in event of network errors. This is an important mechanism to recover from interrupted file transfers rather than simply trying to download the entire file again.

7.2.2.3. Efficient Traffic Usage

- Caching: Keep a copy of the portion of data that has already been downloaded, in case it is needed again. Caching can reduce the need to reload images, web pages, style sheets, etc. which results in fewer data transfers, reducing network signalling and make apps appear faster and more responsive.
- Cloud based transformations: Avoid aggregation and processing of data from multiple data sources on the mobile application client. Instead perform these operations on an application server and expose its functionality as a web service via APIs to minimise the number of network connections and data transfer to the client.
- Media transcoding: Content optimisation can minimise data usage and reduce download times. Developers should utilise the OS platform APIs/User Agent information to determine the device capabilities regarding screen display resolution and streaming capabilities and serve media accordingly. The lowest resolution/frame rate/codec rate that gives a good user experience should be used. Application Server should also have media content encoded in a variety of bit rates and the app should choose the media rate that suits the radio network being used.
- Presence: To minimise unnecessary traffic from presence based services information on presence or availability of users should be bundled before being published instead of sending/requesting an update per user separately. Make use of partial publication to only update information which has changed since the last state.
- Email: Consider imposing maximum attachment and message size limits to reduce the amount of data transfer. Provide users with a choice to download large attachments/messages instead of doing so automatically. Make use of Push notifications from server to device instead of polling to update messages.
- Push notification: Many applications attempt to deliver real time news, notifications and other data to devices by periodically polling the network which is wasteful if there is no new information on the server and causes unnecessary network signalling and drain on device battery. Instead push data to the device when there is actually new and relevant information available.

- Compression: Data compression where possible can be used to minimise data transferred over the network and reduce costs for the user. Applications that are text based and use HTTP protocols such as news aggregators lend themselves well to compression techniques, which can reduce text data size by 80%.
- Data batching: It takes time, power and network signalling to switch between device RRC (Radio Resource Control) states. When a device switches from an idle to dedicated channel to send data it may consume 60-100 times the amount of power it does in the idle state. By batching data, we save on these state changes, reduce battery drain and network signalling (which is beneficial for other network users). Batching applies on both the uplink (device to network) and downlink (network to device) sides.

7.2.2.4. Background Mode

Background mode refers to when the user interface of the application is not visible to the user and the app is not actively being used, in a multitasking environment. Once an app is placed in the background, the user might reasonably expect the app is not doing any data transfers. This however is not always the case.

Avoid network chattiness for your app in background mode – unless it is very clear to the user that the app will still work in background mode.

Cease relevant activity of app when it is placed in background e.g. stop video/ audio streaming , network connection and so on until app is brought into the foreground but continue other activity that might be required e.g. keep track of videos user has watched etc.

Give user an option in the app settings to stop app data transfer in background use. Some apps continue to run when in the background including transferring data which might not be what the user wants.

7.2.2.5. Application Scaling

Scale the application's network activity and behaviour depending on the available power reserves and network conditions to extend battery life and provide a good user experience.

App should be developed to scale functionality according to the capabilities of the network it is connected to. More data intensive functions of the app should be limited to meet available network throughput. For instance:

- When on 3G, consider restricting video streaming functionality as the network speeds will not be sufficient to support video at high quality.
- Scale back the codec rate of video delivered when connected at lower speeds but offer higher quality video streaming and image resolution when on the faster 4G network or Wi-Fi.

To extend device battery life, app activity should be ratcheted down as battery charge declines. Some possible app activities that could be scaled are:

- Reduce periodicity / frequency of app updates or polls as battery declines.
- Reduce retry algorithms in low battery situations to not hasten a flat battery
- Do not allow certain activities without user warning and acceptance
- E.g. once battery reaches a certain limit, do not allow certain activities such as uploads / downloads of large files, streaming, GPS activation etc. Inform user that

battery is low and connection to a charger is recommended to continue activity (allow user to override however).

Device battery life can be extended by deferring non time critical uploads/downloads until charging. Consider settings options for your app to only upload / download large files such as captured photos and videos when charging.

7.2.2.6. Network identification

It is not uncommon for application developers to identify which specific network a device is connected to and for application programs to take different actions based on the network the device has attached to. Network operators transmit identification information in both numeric and alphanumeric formats.

The use of numeric information shall always be the preferred format. That is, numeric format provides the network operator's Mobile Country Code (MCC) and Mobile Network Code (MNC) which remains stable whereas the information provided in alphanumeric format is a textual string which can and does change from time to time. For further information, please refer to the "+COPS parameter command syntax" and "informative examples" in sections 7.3 and 7.45 respectively within 3GPP Technical standard TS27.007 https://www.3gpp.org/DynaReport/27007.htm, select the Version tab then the latest Version number.

7.2.3. References

Guides for Android and iOS platforms are below:

Google Android:	Connection management https://developer.android.com/guide/topics/connectivity Push notification https://firebase.google.com/docs/cloud-messaging/ Battery State http://developer.android.com/reference/android/os/BatteryManager.html
Apple iOS:	Connection management https://developer.apple.com/library/archive/documentation/NetworkingInternetWeb/Conceptual/NetworkingOverview/Introduction/Introduction.html Push notification https://developer.apple.com/library/archive/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/APNSOverview.html#//apple_ref/doc/uid/TP40008194-CH8-SW1 Battery State http://developer.apple.com/library/ios/#documentation/uikit/reference/UIDevice_Class/Reference/UIDevice.html

7.3. Network Connection Efficiency

7.3.1. Description

Mobile applications should consider the frequency and timing of their network connection establishment. Mobile devices need to transition through different devices states of increasing power draw and initiate several signalling events to setup a connection with the mobile network for transfer of application data. Misbehaving applications can be disruptive to the network and pose a significant drain on device battery.

7.3.2. Methods

7.3.2.1. Use Conservative Retry Algorithms

Conservative retry algorithms are required to prevent apps from continually trying to upload or download content in the event of end-to-end connectivity failures such as server issues, time-outs or slow network speeds. This is to prevent rapid battery drain and reduce harm to other network users.

Key principles include limiting aggressive retry attempts, sensible back off timers and finite retry algorithms.

A sensible retry algorithm will have a randomised back off time (before retry), with increasing time between retries and a finite number of retries before indicating failure to the user/application.

In an IoT/M2M application, conservative retry algorithms are critical. Consider the utility IoT/M2M monitoring case where thousands of IoT/M2M devices might concurrently try to reconnect to their server after a power outage to upload their measurements. Without a well designed retry algorithm, this can cause network access congestion, affecting not only the M2M specific application but other network users.

Another consideration for IoT/M2M applications is the effects an unsuitable retry algorithm could have on the battery life of the device. The importance of getting the device back online as soon as possible needs to be weighed up against the power requirements of having a more aggressive retry algorithm.

7.3.2.2. Avoid Synchronised Access to the Network

Smartphones and tablet devices are often synchronised to a common central clock. If multiple apps use absolute times to synchronise simultaneously to perform actions like fetch email or news updates, they may cause blocking at the local cell level or create excess load across the entire network.

IoT/M2M devices are typically deployed in large numbers with many sharing common network access points in the form of the local mobile base station. If all these devices were to attempt to signal the network simultaneously it would create a lot of congestion.

To avoid synchronised app access to the network, activities shouldn't be scheduled for the exact same absolute time across large applications. In an IoT/M2M scenario, we would not want all smart meters reporting for a utility to occur at exactly the same point in time across an entire city. Similarly, we would not want an email client set to check email at exactly 8am each morning.

Developers should consider spreading /randomising device access by random offsets that are relative to the nature of the activity. For instance, for a periodic IoT/M2M activity that requires a small transfer to occur hourly, spread the accesses for the devices randomly across the hour.

For something large such as a large software/firmware update consider randomising device updates over a longer period such as week or a month and consider doing the data transfer at an off peak time such as in the middle of the night between midnight and 6am.

For IoT/M2M solutions make sure you consider the case where a power outage (for devices that use mains power with no battery back-up) results in all the devices powering back up at the same time. These devices should not all try to reconnect to the network at the same time. Stagger the network activity of all the IoT/M2M devices so as not to contribute to network congestion. A similar approach to stagger network reconnection activity should be used when recovering from a network outage or other loss of connectivity. Eg. Cloud server failure

Note Telstra's terms and conditions also mandate conditions around synchronised access to Telstra's network for multiple IoT/M2M modem devices and contains the following clause "If your Wireless M2M application employs more than 50,000 modem devices, you must provide a facility to control data transmission intervals in real time. We may require you to increase data transmission intervals during periods of network congestion".

Link to Telstra's "Our Customer terms"
https://www.telstra.com.au/content/dam/tcom/personal/consumer-advice/pdf/business-b/dataservices-m2m.pdf

Developers should not schedule periodic reboots / power cycles of their devices. That is, do not do a daily reboot of the IoT device to make sure you have a fresh connection setup. A behaviour that imposes strain on the network as it generates a large volume of network signalling and the more devices in use, the greater the load on the network. If device resets are required, then as described for software/firmware updates the resets should be randomised over a long period , a week or a month and they should be performed at off peak times such as between midnight and 6am.

A good practice is for each end device to forward radio cell identity details to the centralised IoT/M2M management platform controlling the application or devices. This will allow the application platform to understand how many devices for that application are located in specific cells. The application platform can then modify the device configuration parameters controlling the rate at which devices send data or reconnect to the network as well as the time duration over which these activities are randomised. For example, the setting of configuration parameters for a radio cell would be significantly different if there were 3, 30, 300 or even 3000 devices operating in the very same radio cell.

7.3.3. References

See Section 7 – Connection Efficient Requirements from GSMA IoT Device Connection Efficiency Guidelines v7.1:

Refer "Use of multiple modem devices" in Telstra's Our Customer Terms.

https://www.telstra.com.au/content/dam/tcom/personal/consumer-advice/pdf/business-b/dataservices-m2m.pdf

7.4. Firmware over the Air Updates

7.4.1. Description

Firmware over the Air (FOTA) upgrade is the ability of a device to have its firmware/operating system and RF chipset firmware upgraded using the cellular network ("over the air").

Note FOTA can be achieved by proprietary methods or standardised methods such as described by OMA (Open Mobile Alliance) Specifications body (http://openmobilealliance.org/) in which case it is using the OMA-DM (OMA Device Management) standard on FUMO (Firmware Update Management Object) or LwM2M (Lightweight M2M). Telstra has no preference for method used. Telstra expects the vendor/OEM or integrator to host the FOTA server for their devices.

Device vendors should keep up with latest OS and/or module firmware releases, rolling out updates as they become available to ensure new security vulnerabilities are addressed and known issues are minimised.

From time to time, you, your manufacturer or supplier may need to implement upgrades to your devices due to Telstra network upgrades. If these upgrades do not occur, devices may no longer work. Where possible, Telstra will give your reasonable notice when an upgrade is required. Vendors need to proactively monitor updates and release notes from their suppliers to determine when a FOTA update is required and the urgency this shall be released with. If you are unclear whether a device firmware upgrade is required, please contact Telstra for guidance. Upgrading the device firmware may result in the device being certified again for use on the Telstra network.

Note that Telstra reserves the right to insist on a firmware upgrade using this capability at any time should we find device issues causing network harm/other user harmful impacts.

7.4.1.1. For IoT/M2M devices and applications

FOTA capability is extremely important for IoT/M2M devices given the:

- Large number of devices in remote or hard to access locations
- Longer lifecycle / lifespan of these devices compared with smartphones. FOTA is important because if any bugs are found in the device while in the field, or any future incompatibilities are found between the device and our radio network, these can be remotely rectified by the vendor/manufacture.

One of the main principles prioritised by the Australian Government's code of practice for securing Internet of Things devices, (https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf) is the need to keep software securely updated. Organisations deploying IoT/M2M devices and manufacturers/developers of IoT/M2M products and applications need to realise it's not a case of if the device's firmware will need a FOTA update during it's lifetime but when will it be needed and how regularly. The software and firmware in mobile handsets is updated at regular intervals. Just because an IoT/M2M device is not held in someone's hand, does not mean it's immune from requiring updates. It is an unrealistic expectation for IoT/M2M devices to be deployed into the field and for them to never require an update.

When deploying devices at scale, an environment and accompanying procedures needs to be developed to easily, securely and reliably update those devices. For example, it is not uncommon for security reasons to see devices deployed into a private APN with no access to the

greater internet. In such a case, how can those devices be updated over the air without compromising the security arrangements put in place? Techniques and methods required to update these devices in secure private APNs need to be planned from the outset, prior to device deployment. With zero day and other similar exploits becoming more prevalent, taking 12-18 months to determine and develop procedures to safely update a fleet of IoT devices is not a satisfactory approach. This requirement to support timely firmware updates extends to not only devices deployed in the field but devices held in warehouses ahead of deployment to the field. Deploying a device into the field with a known issue and hoping you can update it once the device is in situ, is not a sound practice.

For IoT/M2M developers seeking Telstra endorsement of their IoT/M2M device or solution, it is mandatory that there is a mechanism to update the firmware of both the cellular modem and the software of the integrated device remotely. That mechanism needs to be able to support deployment at scale. Mechanisms that work in a lab environment for 1 or 2 devices but don't scale to support 1000s of devices, are not acceptable. In some rare cases exceptions may be made and other mechanisms for upgrade may be allowed e.g. fixed internet connectivity, Wi-Fi, cabled connection.

7.5. Design with IPv6 Transition in Mind

7.5.1. IPv6 Requirements Discussion

Telstra is committed to implementing the IP version 6 protocol (IPv6) for communication with mobile devices connected to its network due to IPv4 address exhaustion.

Telstra is progressively enabling APNs for IPv6 use.

7.5.1.1. APN Usage Requirements

The **telstra.wap APN** (used for Handheld and Tablet on device internet access) is IPv4v6 dual stack enabled (supports IPv4 SS, IPv6 SS and IPv4v6) and the network path includes a NAT64.

New handheld and tablet devices using the **telstra.wap APN** shall be configured as **IPv6 SS** (Single Stack) for domestic usage (and IPv4 for roaming, as the visited network may not support IPv6).

464XLAT / CLAT functionality is expected on the device for handheld/tablet IPv6 SS usage. Devices without 464XLAT support shall be configured as IPv4 SS for domestic use and IPv4 SS for roaming usage.

The **telstra.internet APN** (mainly used for mobile broadband and handheld/tablet tethering APN) is also enabled for IP4v6 Dual Stack usage. Devices using **telstra.internet** shall normally be configured as **IPv4v6 DS** (Dual Stack) for domestic usage (and IPv4 SS for roaming as the visited network may not support IPv6).

M2M/IoT related APNs and IOT platforms are being progressively IPv6 enabled. Check with Telstra regarding IPv6 support of the APN and IoT platform intended to be used for your device and service.

M2M/IoT developers should use IPv6 capable devices and design end to end service to work as IPv6 SS.

7.5.1.2. Device IPv6 Configuration Requirements

7.5.1.2.1 IPv6 Configuration – Smartphones & Tablets

Telstra requires handhelds and tablets to support IPv6 with 464XLAT capability.

Devices shall be configured as IPv6 SS for domestic use (and IPv4 SS for roaming case, as the visited network may not support IPv6).

Note Android has supported 464XLAT functionality for many years (since Android version 4.2).

7.5.1.2.2 IPv6 Support – IoT/M2M

Telstra requires new IoT/M2M devices to support IPv6 natively.

Telstra requires new IoT/M2M applications and end to end services to support IPv6.

IoT/M2M shall be configured as either IPv4v6 DS or IPv6 SS dependant on the end to end IPv6 enablement of the APN, M2M platform capability and end to end application.

Telstra can be contacted by email at TelstraWirelessM2MHardware@team.telstra.com to discuss APN and IoT platform IP protocol support if needed.

Telstra expects future large-scale deployments of IoT/M2M devices will be configured to use IPv6 only (single stack).

New Telstra Approved/Certified modules are required to support IPv6.

7.5.1.2.3 IPv6 Support – Wireless Broadband Devices

Wireless broadband devices (USB dongles, Wi-Fi hotspots, gateways) are required to be configured as IPv4v6 dual stack for domestic use (and IPv4 SS for roaming case, as the visited network may not support IPv6).

7.5.2. IPv6 Development Guidelines

Some basic app guidelines for IPv6 are:

- Don't hardwire IPv4 addresses in to your app / app code – use variables to represent IP addresses.
- Ensure when coding to use a variable for IP addresses that can hold an IPv6 address
- Ensure apps are both IPv4 and IPv6 compliant
- For IoT/M2M solution developers - use IPv6 SS (Single Stack) and IPv4v6 DS (Dual Stack) capable modules in your device. IPv6 capability will help future proof your device/application – increase its longevity and increase its security (if new security features of IPv6 are utilised).
- Developers using servers as part of their application should ensure that their servers are IPv6 SS (single stack) and IPv4v6 DS(dual-stack) enabled. The application should be designed to work using IPv6 SS end to end (or at least IPv4v6 Dual Stack)

7.5.3. IPv6 References

7.5.3.1. IPv6 General Reference

https://www.internetsociety.org/deploy360/ipv6/faq/

Refer to Appendix B:of this document for an explanation of IPv6 terminology

7.5.3.2. XLAT464 References

https://datatracker.ietf.org/doc/html/rfc6877

Refer to RFC7849: An IPv6 Profile for 3GPP Mobile Devices for recommendations on connecting to IPv6 networks while also ensuring IPv4 service continuity
https://datatracker.ietf.org/doc/html/rfc7849

7.6. Follow Security Guidelines

7.6.1. Description

Developers need to consider security and privacy aspects of their application to protect their users and their user's data.

Developers need to consider the following when developing applications

- Credential management – whereby default/initial username/password needs to changed at first use
- Security of user's sensitive information
- Fraud Prevention
- Provide an OTA (over the air) software/firmware update mechanism – so any identified security issues can be quickly patched
- Certificate management

7.6.2. Methods

Some methods developers can employ to ensure the security of their application, solution and its data:

7.6.2.1. General Guidelines:

- Use the respective OS platform's app store update mechanism to address any app security issues ASAP
- Do not store or send user passwords or any other sensitive information in unencrypted text
- Use secure protocols such as SSL/TLS for transmitting any sensitive information over the network
- Enforce higher security password requirements on the user. e.g. A mixture of upper & lower case, alpha numeric & special symbols and lengths > 8 characters
- Ensure that no sensitive information is stored in the app log files
- Test the app to ensure that passwords / authentication cannot be bypassed
- Minimise app platform permissions to only the absolute minimum necessary so as to minimise vulnerabilities and increase user confidence
- Developers should use well known standardised security libraries / third party software APIs that provide security/encryption functions that have been well tested in the market (and hardened/patched against known vulnerabilities)

- Note many of the platform OS security protections can be circumvented by 'jail breaking' or 'rooting' the device – so ensure that app code uses its own security mechanisms beyond those provided by the OS platform.
- Developers should only distribute their app via the official OS platform's app store and not make the app package available for distribution elsewhere. Malicious code can be inserted into standalone versions and redistributed versions of the app can leave users vulnerable to identity theft and various forms of malware.
- Conduct penetration testing of the solution to identify vulnerabilities that need to be addressed

7.6.2.2. IoT/M2M Application Specific Guidelines

Security cannot be trivialised – especially considering some of the main applications of IoT/M2M. The impact of security and hacking breaches can be extremely serious.

Applications and solutions need to consider security as a key design principle. A good starting point is alignment with the Australian Government's code of practice for securing the Internet of Things. https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

IoT/M2M devices are key to emerging industries such as smart grids and health monitoring. Needless to say, security (and privacy) breaches in these cases could have life threatening and wide spread community impact.

Security is also needed for fraud prevention – given that these devices and their SIMs may be relatively accessible in high numbers.

Some specific security measures for IoT/M2M devices include:

- Firmware update capability (OTA) to allow device to be quickly patched should any security issues / vulnerabilities come to light.
- Ensure the physical security of the SIM in the device. For instance, to avoid the oft-cited scenario where utility meters sim cards are stolen and used for data/call theft.
- Use IPv6 - due to its enhanced security features
- Utilise vendors FOTA to ensure you have the latest firmware for your device
- Review module and OS development platform security guidelines
- Ensure device has sufficient password protection / user authentication procedures to prevent against hacker access
- The physical security of devices when installing. Consider alarming device back to central server e.g. alarm if enclosure is opened
- Utilise external consulting/testing expertise against hacking/intrusion for critical IoT/M2M applications in utility and health monitoring areas.
- Consider hiding SSID for Wi-Fi connected devices. No need to broadcast.

7.6.3. References

7.6.3.1. OS Platform Security Guidelines

Each of the major mobile OS platforms has its own security guidelines for developers. These are a very good reference for developers.

Google Android: https://developer.android.com/privacy-and-security/security-tips

Apple iOS: https://developer.apple.com/library/mac/documentation/Security/Conceptual/SecureCodingGuide/Introduction.html

Android Developer Security Tips (whilst specific to Android contains principals that are applicable to all platforms):
https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide/Introduction.html

Telstra strongly encourages developers to review and align with the following guidelines where appropriate for the product or service being offered:

Code of Practice for Consumer IoT Security	UK Government - Department for Digital, Culture, Media & Sport	https://www.gov.uk/government/publications/secure-by-design
Internet of Things Security Guidelines	IoT Australia Alliance	http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf
GSMA IoT Security Guidelines and Assessment	GSMA	https://www.gsma.com/iot/iot-security/iot-security-guidelines/
CTIA IoT Cybersecurity Certification Program Management Document	CTIA	https://api.ctia.org/wp-content/uploads/2018/10/ctia_IoT_cybersecurity_pmd_ver-1_0.pdf
Australasian Information Security Evaluation Program	Australian Cyber Security Centre	https://www.cyber.gov.au/resources-business-and-government/assessment-and-evaluation-programs/australian-information-security-evaluation-program
Code of Practice - Securing the Internet of Things for Consumers	Department of Home Affairs	https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf
Cyber Security for Consumer Internet of Things: Baseline Requirements	European Telecommunications Standards Institute (ETSI)	https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

7.7. Follow Privacy Guidelines

7.7.1. Description

Telstra respects user's privacy and it is important that developers ensure users privacy. There are legal penalties for not following the applicable laws.

7.7.2. Methods

- Ensure that no user information is sent to third parties without the user being clearly informed and opting into the service (they must be clearly informed of where the data is going and how it will be used)
- GPS should not be used without the users consent to track / record user location
- Ensure security guidelines above are adhered to as these will help safeguard the users privacy
- Ensure your app complies with Australian Privacy Laws.
- Consider what data is collected, how long it needs to be retained and how to safely dispose of the data when no longer needed.

7.7.3. References

Australian Privacy Laws: https://www.oaic.gov.au/privacy/the-privacy-act/

7.8. Coverage

Whilst for handheld and tablet devices, an end user can readily view the screen and assess the level of coverage at a given location, for IoT/M2M devices operating in remote locations, it's not so easy to assess the level of network coverage at a given location.

For IoT/M2M applications it is good practice for the end device to report to a centralised device management platform, the reference signal receive power (RSRP) and signal to interference plus noise ratio (SINR). If these measures are included with each report, it is possible to observe the coverage performance at a location and how that coverage varies over time. For example, large drops in signal strength may be indicative of a vehicle parking alongside the end device and obscuring coverage. Alternatively, it could also indicate a loose antenna connector. Similarly, it may be useful in understanding a poor experience when localised noise sources may be interfering with the end device.

In addition to signal conditions at a specific location, it is also worthwhile for an application to report the identity of the cell providing that coverage. This information can help in identifying issues where for example an installer points a directional antenna at what they think is the best base station, only to find the radio signal in the area is coming from another base station in a different direction to where the antenna is pointing

The cell ID can also be useful where for example, a smart metering company may have deployed many meters in a given region. By knowing the identity of the cell providing coverage, the metering company will know whether for example, they have 3000 meters in a single cell or 300 meters in each of ten different cells. This information is particularly useful when the meters need to be polled, provided with firmware updates over the air or avoiding other situations

where those meters may act in unison and congest a radio cell. Remembering that a single metering company may not be the only user with large numbers of devices in that region.

7.8.1. Power class

One of the easiest ways for an application developer to impact the coverage performance of a device is to build that device using a lower power class radio.

Cellular radios have a maximum power output at which they transmit signals. Noting that this is the maximum output level the radio can achieve but may not be the actual power output it uses at a specific location. That is, a cellular radio will adjust its power output to suit the radio conditions. In good coverage it may only use a fraction of its output power whereas in poorer coverage conditions, it may be transmitting a signal at full power.

Cellular radios with different maximum power outputs are grouped into what's called power classes with each power class representing different maximum power outputs. Smartphones and many radio modules in market are power class 3 devices. They can transmit at a maximum output power of 200mW (+23 dBm).

It is possible to purchase power class 5 or 6 IoT radio modules. These radio modules have a maximum power output of 100mW (+20dBm) or 25mW (+14dBm) respectively. By having a lower maximum power output than power class 3 radios, power class 5 or 6 radios are unable to provide the same depth or breadth of coverage as the power class 3 radio normally used by most cellular devices.

Lower power output radios may appear attractive due to perceived lower power drain for battery powered devices or lower cost. A reduction in output power may mean a mobile IoT device enters increased Coverage Enhancement levels sooner than a power class 3 device. The impact may mean for some devices, any energy savings gained through reduced power output are lost or exceeded by the signal repetitions required to deliver a message. Sitting side by side with a lower power output radio, a power class 3 radio should reduce its power output to the same as the lower power output radio.

Application developers should carefully consider the coverage impact that may be experienced using a lower powered radio. Whilst selecting a slightly lower cost item may seem attractive, depending on where or how the radio is used, it could lead to higher customer care costs and increased customer dissatisfaction if customer coverage expectations are not realised. It needs to be remembered that the Power Class defines the maximum power output and depending on the coverage, a mobile IoT device may be operating well below the maximum power output level anyway.

Telstra strongly recommends use of Power Class 3 devices. This is likely to provide an optimal experience for the end customer.

7.8.2. In building coverage

Another way to impact the performance of a radio device is to place it inside a building. Depending on the construction materials used for the building, the radio signal available to the device may be significantly impacted. For example, for large multi-story buildings, it is common for reinforced concrete to be used. Radio signals passing through these structures will have their signal strengths reduced, the amount of reduction depending on both the thickness and density of the concrete, the arrangement of the reinforcing mesh and the operating frequency in use.

Generally, low frequency signals experience less signal attenuation as they pass through building structures than higher frequency signals. That is, the 700 MHz frequency band typically experiences less signal attenuation than the 1800 MHz frequency band.

The location of the device within the building may also impact it's performance. With mobile radio signals typically provisioned to meet the needs of users near the ground, a device located atop of a 40 story building or below ground level in a basement, may experience poor performance.

Recognising the impact building construction may have on radio coverage, some property owners have installed in building coverage systems. These systems typically operate on the 1800 MHz or 2600 MHz bands. Therefore, IoT services operating on 700 MHz do not experience the improved coverage of the in building coverage system.

A consequence of which, placement of devices within buildings may need to be carefully considered if the devices are to operate successfully. That is, installers should check that there is coverage from the network for the required band at the specific install location to ensure device connectivity.

7.9. Conclusion

In conclusion, developers should consider the guidelines mentioned throughout this section.

One thing to bear in mind is these general principles apply to both data transfers and signalling that occurs due to network accesses and detaches.

There should be randomisation, sensible back-off algorithms and non-infinite retries for all types of network use - both data transfer and network accesses. Network cause codes and device behaviour is highly relevant to this and details some common network cause codes and how devices should behave upon receiving them.

8. APPLICATION TESTING

8.1. Importance of Testing:

One of the most important aspects of app development is testing.

Testing prior to deployment has obvious advantages -

- Less chance of significant errors being found by users
- Ability to tune app performance
- Ability to observe network interoperability performance
- Ability to tune device battery performance
- Ability to observe any unintended behaviour and rectify

8.2. General Testing Guidelines

- Field testing of the app should be performed rather than just using a simulation tool.
- App should be tested on all networks it could end up on i.e. 3G, 4G, 5G and Wi-Fi. Performance differences should be noted and code optimisation done as a result.
- App should be tested in areas with poor coverage / network connectivity to see how robust / resilient the app is to poor network conditions and connectivity and whether further app optimisation is required to account for these issues.
- App should be tested in peak times (for data apps typically around 9pm on a weekday) to see how it performs under busier network conditions where there may be additional delays in responses from network.
- App should be tested against any user configurable settings that are possible i.e. if user can set times for push to be disabled – check that these actually are disabled at the set time, or if uploading of photos is only permitted on Wi-Fi, make sure that this occurs.
- Monitor battery usage with the app (most operating systems provide battery monitoring tools and app stores have battery monitoring apps).
- Monitor data usage of the app. Check that it is consistent with expectations.
- Ensure app server responds as expected in all the different test cases and network conditions as possible.
- Try as many different combinations of usage cases as possible to detect any unintended UI behaviour.
- Try to test using a variety of device models to ensure your app caters properly for different screen types, resolutions, device types (tablets vs. handsets)
- Consider using an external test house that has a large selection of devices or use crowdsourcing web sites to get beta testers using a variety of devices.
- Use User Agent switchers on desktop browsers to see how mobile web sites will be rendered on different devices.
- Check app behaviour with no network connectivity (offline). Does it provide access to functionality that doesn't require a network connection or does it hang?

- Check that app performs as expected when in airplane mode or without a sim (i.e. no network connectivity)
- Test performance after network connectivity is restored after losing it.
- Check that app performs as expected when there is a cabled connection to computer (tethered)
- Check interaction with peripherals such as SD card, Bluetooth accessories.
- Check that app performs as expected with above peripherals on/off/connected/not connected as appropriate.
- Check that app gives user appropriate indication of network connectivity, error conditions and ensure that there is a non-blocking UI. e.g. If no network connectivity the device doesn't flash up an error message and get stuck but rather allows the user to continue with activities within the app that don't require network activity.
- Ensure Security is tested. e.g. user authentication works as expected
- Does the app correctly handle interruptions e.g. from incoming calls.
- CPU usage of app is not excessive (most operating systems provide CPU monitoring tools)
- That the app performs as expected when the device is multitasking with other apps or when the app is background mode.

8.3. IoT/M2M Specific Testing Guidelines

Given the remote locations and rugged environments that IoT/M2M solutions can exist in testing must be all the more rigorous.

In addition to the testing described above the following additional testing is required for IoT/M2M:

- Test that FOTA solution works – test that both the application software can be updated and verify that firmware upgrade solution will work.
- Test that device is sufficiently rugged for planned deployment/usage. Is the device sufficiently hardened for the expected environment?
- Test for heat, vibration, moisture, UV exposure and generally adverse weather
- Test for failure conditions e.g. for power metering application, what happens if there is a power failure or recovery from a loss of connectivity? Does your reconnect algorithm randomise and back off connection attempts to handle deployment at scale?
- Test that device over the air diagnostics work
- Verify that network reacquisition and retry algorithms function in a finite and non-aggressive way
- Test IPv6 functionality

8.4. References

http://www.appqualityalliance.org/online_testing_tool_and_best_practice_update

APPENDIX A: TELSTRA WIRELESS AND IOT/M2M RELATED PRODUCT INFORMATION

A.1 Telstra Mobility Partners

Telstra has dedicated product and solution teams to assist developers with integrating IoT/M2M solutions on our network. Email TelstraWirelessM2MHardware@team.telstra.com for assistance.

A.2 Telstra IoT Offerings

https://www.telstra.com.au/business-enterprise/products/internet-of-things

A.3 Telstra IoT Platform

https://www.telstra.com.au/business-enterprise/products/internet-of-things/capabilities/cumulocity

A.4 Telstra IoT Connection Management

https://www.telstra.com.au/business-enterprise/products/internet-of-things/capabilities/connection-management-platform

A.5 Telstra Mobile Assets and Workforce Enterprise Solutions

https://www.telstra.com.au/business-enterprise/solutions/mobility-solutions

A.6 Telstra Wireless Managed Data Networks – Wireless WAN

https://wirelesscommunications.com.au/wp-content/uploads/2016/10/Telstra-Managed-Data-Networks.pdf

A.7 Telstra IP VPN information

https://www.telstra.com.au/business-enterprise/solutions/network-services/connectivity/vpn-service

A.8 Telstra Enterprise Support Contacts

https://www.telstra.com.au/business-enterprise/contact-us

Telstra Mobile Phones https://telstra.com.au/mobile-phones

A.9 Telstra Mobile Coverage

https://www.telstra.com.au/coverage-networks/our-coverage

A.10 Telstra IoT Coverage

https://www.telstra.com.au/business-enterprise/about-enterprise/our-network/iot-coverage-map

APPENDIX B: IPV6 DESCRIPTION AND TERMINOLOGY

The drivers for the use of IPv6 and the description of IPv4 exhaustion have been well documented on the Internet and will be assumed to be understood by device application developers.

IPv4 and IPv6 are distinct protocols that do not natively interoperate but it can be assumed that both protocols will need to coexist in the Internet for many years to come. This means that any device will need to communicate with other devices that may themselves either speak only IPv6 or IPv4, either by itself natively speaking both protocols ("dual stack" configuration) or through a protocol translator or tunnel in the network or the device (e.g. NAT64, 464XLAT, etc.).

B.1 Single Stack

A single stack network or device as the name implies only supports a single IP protocol type. Single stack is often denoted simply as SS.

There are two possibilities:

1. IPv4 SS network, supporting only IPv4 traffic as most existing wireless networks are today
2. IPv6 SS network, supporting only IPv6 traffic

B.2 Dual Stack

A dual stack network is a network whose nodes are capable of processing IPv4 and IPv6 traffic simultaneously. It thus facilitates the transition to IPv6 while many devices and internet sites are still IPv4 by letting the two protocols co-exist.

A dual stack UE (user equipment aka mobile device), supports the following PDP types IPv4 (single stack), IPv6 (single stack) and IPv4v6 (dual stack or "DS" – that is an IPv4 and an IPv6 connection simultaneously).

A dual stack UE will request a dual stack bearer (IPv4v6) and the network will allocate the appropriate bearer which may be either IPv4 single stack, IPv6 single stack, or dual stack (both an IPv4 and IPv6 connection).

B.3 464XLAT

For handsets & tablets that are IPv6 single stack capable there will still be a need for many years to co-exist with the IPv4 ecosystem. E.g. to reach IPv4 sites, or for apps that are not yet IPv6 compatible (i.e. contain IPv4 literal addresses within their code).

RFC6877 464XLAT provides a solution to allow IPV4 services & applications to work over an IPV6 single stack network. The 464XLAT solution requires at a minimum a NAT64 in the network along with 464XLAT daemon/code running on the device.

464XLAT refers to architecture for both network and device to allow this to work and this is described in RFC6877. Refer http://tools.ietf.org/html/rfc6877. The 464XLAT code required by the device is open source code and is available to be used in any operating system.

APPENDIX C: NETWORK CAUSE CODES AND DEVICE BEHAVIOUR

The network has a variety of cause codes that it can send to the device in response to device requests that indicate a reason for failure of the request.

The device should pay attention to these cause codes and behave accordingly.

In a few cases the industry (3GPP) specifications and network timers specify the retry algorithm's behaviour but not always completely. Thus, in these cases and where not specified at all, the behaviour is left to the device manufacturer/integrator. As discussed earlier, if retries are required, they should not be aggressive and infinite in nature.

Some cause codes indicate trouble with a user's service subscription and retries are pointless (once issue is confirmed as not a one off) – in this case the user/developer needs to confirm their service subscription status with Telstra. For 3G these cause codes are described in 3GPP specification 24.008 annexes.

Refer http://www.3gpp.org/DynaReport/24008.htm

There are three main categories of error codes. Those related to Mobility Management (MM), Call Control (mainly applicable to voice calling) and Data Session Management (SM).

Mobility Management (MM) includes causes related to:

- MS Identification,
- Subscription Options
- Network Failures/Congestion/Authentication Failures
- The nature of request
- Invalid messages
- GMM = related specifically to data

Call Control (CC) causes are grouped into:

- Normal Class
- Resource unavailable class
- Service / Option not available
- Service Not implemented class
- Invalid Message
- Protocol error
- Interworking issues

GPRS/Data Session Management (SM) [ESM used for LTE] are divided in to subgroups of causes related to:

- Nature of request
- Invalid Messages

The table below summarises some commonly seen codes, their meaning and suggested device behaviour.

Cause Code	Meaning	Scenario where it may occur	Proposed Device Behaviour or Developer Action Required
8	Operator Determined Barring	Service is barred	Don't retry - contact Telstra Support to ascertain why service is barred.
26	Insufficient resource	Network has insufficient resources e.g. Congested	Since network is congested wait and try again. The device shall not enter an endless retry mechanism. After each rejection, the device shall introduce a back off timer (recommended 12 minutes). We suggest doubling this back off timer after each rejected request and ultimately stop the requests after a period of time (recommended 2 days). Device must still comply with relevant 3GPP standards and obey applicable network timers Consider sending data during off peak times (midnight - 6am)
27	Missing or unknown APN	Incorrectly configured device settings for APN profile	Confirm with Telstra that you have correctly configured and are using the correct APN for the application After each rejection, the device shall introduce a back off timer (recommended 12 minutes). We suggest doubling this back off timer after each rejected request and ultimately stop the requests after a period of time (recommended 2 days).

Cause Code	Meaning	Scenario where it may occur	Proposed Device Behaviour or Developer Action Required
28	Unknown PDP address or PDP type	3G specific analogous to 54 for LTE. Possibly due to incorrect internet destination configured in device	The device shall not enter an endless retry mechanism. After each rejection, the device shall introduce a back off timer (recommended 12 minutes). We suggest doubling this back off timer after each rejected request and ultimately stop the requests after a period of time (recommended 2 days). Device must still comply with relevant 3GPP standards and obey applicable network timers. Developer should check device configuration and internet settings Seek Telstra technical support if error persists
29	User Authentication Failed	Service or SIM error	If this occurs more than once, then contact Telstra Support to confirm service subscription is correct and to investigate the issue.
30	Activation rejected by GGSN, Serving GW or PDN GW	This error occurs if the device/application is requesting a service that is not supported by the network.	Again device shall not endlessly try - but rather stop and provide meaningful error to the user. Developer to investigate what service is being requested and confirm with Telstra whether the service is supported and if not what an equivalent alternative service would be suitable. Again device shall not endlessly try - but rather stop and provide meaningful error to the user

Cause Code	Meaning	Scenario where it may occur	Proposed Device Behaviour or Developer Action Required
31	Activation rejected, unspecified	Possibly due to the requested service option not being subscribed to or other reason	The device shall not enter an endless retry mechanism. After each rejection, the device shall introduce a back off timer (recommended 12 minutes). We suggest doubling this back off timer after each rejected request and ultimately stop the requests after a period of time (recommended 2 days). Device must still comply with relevant 3GPP standards and obey applicable network timers. Contact Telstra for support
32	Service option not supported	Occurs when the network doesn't support the service option.	Again device shall not endlessly try - but rather stop and provide meaningful error to the user. Developer to investigate what service is being requested and confirm with Telstra whether the service is supported and if not what an equivalent alternative service would be suitable. Do not automatically retry. May occur in a roaming network.
33	Requested service option not subscribed	Occurs due to the requested service option not being subscribed to.	The device shall not enter an endless retry mechanism. The device will not retry unless power cycled or a device setting is altered. Contact Telstra for support

Cause Code	Meaning	Scenario where it may occur	Proposed Device Behaviour or Developer Action Required
34	Service option temporarily out of order	Likely due to network fault	Given that this is due to a network issue that is temporary trying again is reasonable. However, the device shall not enter an endless retry mechanism. After each rejection, the device shall introduce a back off timer (recommended 12 minutes). We suggest doubling this back off timer after each rejected request and ultimately stop the requests after a period of time (recommended 2 days). Device must still comply with relevant 3GPP standards and obey applicable network timers If problem persists contact Telstra for support.
38	Network Failure	Likely due to network outage	Given that this is due to a network failure it is important not to repeatedly retry as this will make it difficult for the network to recover. Suggest backing of for tens of minutes before retrying. As always, the device shall not enter an endless retry mechanism. After each rejection, the device shall introduce a back off timer (recommended 12 minutes). We suggest doubling this back off timer after each rejected request and ultimately stop the requests after a period of time (recommended 2 days). Device must still comply with relevant 3GPP standards and obey applicable network timers If problem persists contact Telstra for support.

Cause Code	Meaning	Scenario where it may occur	Proposed Device Behaviour or Developer Action Required
50	PDP type IPv4 only allowed	Will occur if device requests an IP protocol type (e.g. IPv4v6) that is not allowed by the network or user subscription e.g. if requests IPv6 bearer when they aren't supported	Device shall set up an IPv4 bearer and not request IPv6
51	PDP type IPv6 only allowed	Will occur if device requests an IP protocol type (e.g. IPv4v6) that is not allowed by the network or user subscription e.g. if requests IPv4 bearer on IPv6 Single Stack network	Device shall set up a IPv6 bearer and not request IPv4 bearer
52	Single address bearer allowed		If device requests an IPv4v6 PDP and network sets the PDP type to IPv6 (or IPv4) with cause code #52 (single address bearer allowed), the device shall use the allocated IP address from the network. The device can subsequently request another PDP context activate for the other bearer if it requires dual stack connectivity if the network does not support IPv4v6 on one bearer.
53	ESM Information not received		
54	PDN connection does not exist	LTE specific analogous to 28 for 3G. Possibly due to incorrect internet destination configured in device	Developer should check device configuration and internet settings

APPENDIX D: APN TIMEOUTS

The following timeout info applies to all APNs that undergo NAT (Network Address Translation).

Inactivity timeout for general traffic:

- TCP: 30 minutes
- UDP: 2 minutes
- ICMP: 4 seconds
- DNS: 5 seconds

These timeouts are subject to change.

Extranet services (that do not undergo NAT) have the same timeouts applied TCP/UDP/ICMP/DNS on the stateful firewall.

APPENDIX E: GLOSSARY

Abbreviation / Term	Definition
3G	3rd Generation Wireless Network based on WCDMA technology
3GPP	3rd Generation Partnership Project
4G	4th Generation Wireless Network based on LTE technology standards
5G	5th Generation Wireless Network based on NR technology standards
API	Application Programming Interface
APN	Access Point Name
CA	Carrier Aggregation
DL	DownLink
FOTA	Firmware Over The Air
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
LTE	Long Term Evolution
M2M	Machine to Machine
MB	Megabyte
MIMO	Multiple Input Multiple Output
NR	New Radio
NSA	Non-Stand Alone
OS	Operating System
OMA	Open Mobile Alliance
OTA	Over The Air
PSM	Power Saving Mode
RRC	Radio Resource Control
SA	Stand Alone

SDK	Software Development Kits
SMS	Short Message Service
SSL	Secure Sockets Layer
T&Cs	Terms and Conditions
TLS	Transport Layer Security
UI	User Interface
UL	UpLink
WCDMA	Wideband Code Division Multiple Access

APPENDIX F: DOCUMENT CONTROL SHEET

The purpose of this section is to capture all changes made to the content of document.

Issue No	Issue Date	Nature of Amendment
Version 1	Circa 2005	Initial Document
…	…	…
Version 5	1st Dec 2006	New, rewritten, reformatted version
Version 5.3.3	12th February 2010	Updated network performance information & specifications. Minor corrections & clarifications to network information sections. Repositioned section 10. TELSTRA'S 3G UMTS & GPRS NETWORK ARCHITECTURE for more logical document flow. Updated Telstra web site URLs and removal of obsolete references, particularly sections 18 & 19
Version 6 Draft 1.0	Jan 2013	Completely new version of guidelines – to address both smartphone and M2M applications. Simplification of document
Version 6 Draft 2.0	Mar 2013	Updated based on feedback from Draft 1 reviewers
Version 6 Draft 3.0	April 2013	Updated based on feedback from Draft 2 reviewers
Version 6 Issue 1.0	11th June 2013	Includes changes required for Policy 61 Approval and reformatting to suit new branding template
Version 7 Issue 1.0	30th June 2014	Miscellaneous typo corrections Updated dead/changed URL links Updated references Updated IPv6 sections Updated Telstra LTE spectrum information Added appendix – Network Cause Codes and Device Behaviour
Version 8 Issue 1.0	23rd Mar 2017	Miscellaneous typo corrections Updated dead/changed URL links Updated LTE bands Updated Carrier Aggregation info Removed irrelevant 2G references Added IOT information Updated cause codes to align with MSRs

Version 9 Issue 1.0	21st December 2018	Changed dead URL links Updated network technology and features table Updated LTE device category tables Added GSMA IoT security guidelines reference
Version 9 Issue 2.0	August 2019	Changed 3G longevity statement
Version 10 Issue 1.0	September 2019	Simplified document by removing obsolete, 3G and repeating information Reduced the Application Techniques section, summarising and referencing GSMA and industry guidelines instead Moved mobile network fundamentals and IPv6 explanations to Appendix Updated Telstra Network technology/features and device categories tables Added in more references to IoT throughout the document instead of just M2M Added more information on M2M Control Centre and new section on Telstra IoT Platform Simplified language throughout the document
Version 11 Issue 1.0	July 2020	Updated technology/feature table in section 5.1 Included NB2 in section 5.3.1 & 5.3.5 Updated 3G exit statement in 5.4 Added 5G antenna reference in section 6.3 Added more details on IoT behaviours in Section 7.3.2 General wording updates
Version 12	January 2022	Many updates throughput the document, including further details on FOTA
Version 13	January 2024	General revision