IoT Device Connection Efficiency Common Test Cases

Version 1.0

30 January 2015

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Problem Statement

In Internet of Things (IoT) connectivity scenarios, the IoT Device, IoT Device Application and Communications Module play a significant role in determining the overall performance and behaviour of the IoT service on the mobile network which the device is trying to connect to.

With no human intervention to fall back on, mechanisms that manage recovery from failures need to be built into above software elements of the IoT Device. Poor design of the device, such as any network interactions which disregard the network and device status, may result in inefficient use of network and device resources, affecting the IoT service experience and in some cases, affect network resources such as the Mobile Network's Home Location Register (HLR) or Gateway GPRS Support Node (GGSN) elements.

The IoT Device behaviour when connecting to a Mobile Network shall be verified in order to ensure the best end to end experience and the proper management of the Network resources.

1.2 Document Scope

This document outlines the test cases that would need to be passed by an IoT Device and its incorporated Communications Modules in order for it to be considered compliant with the requirements stated within the GSMA's IoT Device Connection Efficiency Guidelines [1]

The test cases defined in this document form part of a larger IoT Device approval framework as defined in section 2.

1.3 Intended Use of the Document

The target audiences for this document are Mobile Network Operators, IoT Service Providers, IoT Device makers, IoT Device Application developers, Communication Module Vendors and Radio Baseband Chipset Vendors.

1.3.1 Mobile Network Operators

For the Mobile Network Operators this document can be used to provide their customers (any of the players considered in the following sections) with a set of test cases that would need to be undertaken by the customer's IoT Device in order to ensure the customer's IoT Device and IoT Service is compliant with the requirements stated within the GSMA's IoT Device Connection Efficiency Guidelines [1]

1.3.2 IoT Service Providers

IoT Service Providers should ensure their IoT Devices and IoT Services pass the tests defined in this document.

1.3.3 IoT Device Maker

IoT Device Maker's devices are expected to pass the tests defined within this document to prove their devices conform to the GSMA IoT Device Connection Efficiency Guidelines [1].

1.3.4 IoT Device Application Developer

IoT Device Application Developer's applications are expected to pass the relevant tests defined within this document for the IoT Device Application.

1.3.5 Communication Module Vendor

Communication Module Vendor's modules are expected to pass the relevant tests defined within this document for the Communication Module.

1.3.6 Radio Baseband Chipset Vendor

Radio Baseband Chipset Vendor's shall provide chipsets that pass the tests defined within this document when they are integrated into a Communications Module or IoT Device.

1.4 Definition of Terms

See CLNE.03 GSMA IoT Device Connection Efficiency Guidelines [1]

1.5 Abbreviations

See CLNE.03 GSMA IoT Device Connection Efficiency Guidelines [1]

1.6 References

Ref	Document Title	Document Location
1	CLNE.03 GSMA IoT Device Connection Efficiency Guidelines Version 1.1	www.gsma.com
2	GSMA TS.24 “Operator Minimum Acceptance Values for Device Antenna Performance”	www.gsma.com

2 IoT Device Approval Framework

In general, the approval requirements for IoT Devices (and their integrated Communication Modules) fall into three distinct categories:

1. Regulatory Certification. Depending on the vertical market and the geographic area multiple regulatory agencies may be required to be considered for the Communications Module, the IoT Device and even the IoT Device Host certification processes.
2. Industry Certification. In this category we can find telecom industry specific certification schemes, such as Global Certification Forum (GCF) and PTCRB and vertical industry specific certification (for example, in the automotive or utility markets).
3. Mobile operator specific certification/approval process. Mobile network operator certification/approval schemes are typically mandated to ensure the efficiency of IoT Devices operating on the Mobile Operator's Network and to maintain a high level of network performance for the IoT Service Provider's customers. The tests defined within this document will sit within the mobile network operators' specific certification/approval process.

3 Test Environment

The different test environments that can be used for utilizing the tests included in this test case document are:

1. A controlled mobile network (i.e. a live network in a test lab) – see figure 1 below.
2. A simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
3. A 'live' mobile network (i.e. a Mobile Network Operator's live operational network)

Preferably 1) and 2) are to be used since the tester will require some control over the mobile network (radio network and core network) in order to complete many of the test cases. However, to minimize lab testing costs and lab testing time, some preliminary tests using 3), a live radio network together with a specially configured IoT Device can be used to create some of the error conditions (e.g. MM, GMM, SM and SMS errors) necessary to complete some of the test cases contained in this document.

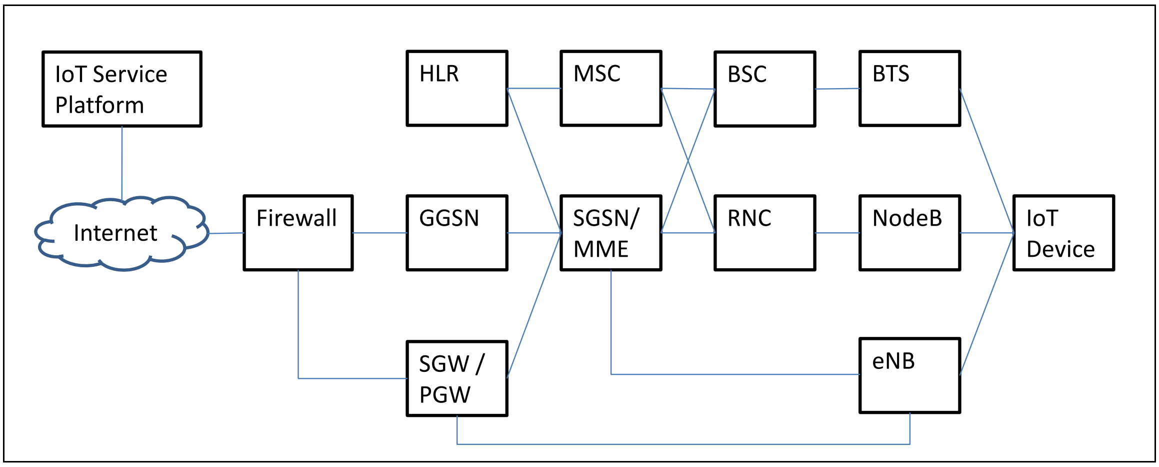

Figure 1: A typical configuration of a 'controlled' mobile network environment in a lab

4 Mapping of Test Cases to Requirements

This section maps the requirements found in the GSMA IoT Device Connection Efficiency Guidelines [1] to the test cases found in section 5 of this document.

IoT Device Connection Efficiency Guidelines Section		Requirement	Test Case	Comments
3	IoT Device Requirements	IDR1	-	High level requirement.
		IDR2	-	High level requirement.
		IDR3	-	See GSMA TS.24 [2].
		IDR4	-	High level requirement.
4	IoT Device Application Requirements	DAR1	TC-DAR1	
		DAR2	TC-DAR2	
		DAR3	TC-DAR3	
		DAR4	-	For future study
		DAR5	TC-DAR5a	

IoT Device Connection Efficiency Guidelines Section		Requirement	Test Case	Comments
			TC-DAR5b	
		DAR6	TC-DAR6	
		DAR7	TC-DAR7	
		DAR8	TC-DAR8	
		DAR9	TC-DAR8	
		DAR10	-	For future study
		DAR11	TC-DAR11a TC-DAR11b TC-DAR11c TC-DAR11d TC-DAR11e TC-DAR11f TC-DAR11g TC-DAR11h TC-DAR11i	
		DAR12	TC-DAR12	
		DAR13	TC-DAR13	
		DAR14	TC-DAR14	
		DAR15	-	For future study
		DAR16	TC-DAR16	
		DAR17	-	For future study
		DAR18	-	For future study
		DAR19	TC-DAR19	
		DAR20	TC-DAR20	
		DAR21	TC-DAR21a TC-DAR21b	
		DAR22	TC-DAR22a TC-DAR22b	
		DAR23	-	
		DAR24	TC-DAR24	
		DAR25	TC-DAR25	
		DAR26	-	For future study
		DAR27	-	For future study
5.1	Standards Compliance	MSC1	-	Out of scope
		MSC2	-	Out of scope
		MSC3	-	Out of scope
5.2	Network Efficiency Requirements	NER1	-	High level requirement
		NER2	-	For future study
		NER3	-	Out of scope
5.3	Requirements for Communication Modules that Support IPv6	IP1	TC-IP1	
		IP2	TC-IP2	
		IP3	TC-IP3	
		IP4	TC-IP4	
		IP5	TC-IP5	
5.4	Requirements for Communication Modules that	CML1	-	Out of scope

IoT Device Connection Efficiency Guidelines Section		Requirement	Test Case	Comments
	Support LTE			
5.5	Requirements for Communication Modules that Support Fast Dormancy	CFD1	TC-CFD1	
5.6	(U)SIM Interface Requirements	MSI1	-	Out of scope
		MSI2	-	Out of scope
5.7	Security Requirements	MSR1	-	High level requirement
		MSR2	TC-MSR2	
		MSR3	-	For future study
		MSR4	TC-MSR4	
5.8	Device Management	DM1	-	High level requirement
		DM2	-	High level requirement
		DM3	TC-DAR24	
		DM4	TC-DAR25	
5.9	Subscription Identifier Requirements	IR1	TC-IR1	
		IR2	TC-IR2	
5.10	Device Host Identity Reporting	DID1 to DID32	-	For future study
6	IoT Service Provider Requirements	MCR1	-	For future study
		MCR2	-	Out of scope
		MCR3	-	For future study
		MCR4	-	For future study
		MCR5	-	For future study
7	Connection Efficiency Requirements	CER1	-	High level requirement.
		CER2	-	High level requirement.
		CER3	-	High level requirement.
		CER4	-	High level requirement.
7.1	Network Friendly Mode	NFM1	TC-NFM1	
		NFM2	TC-NFM2	
		NFM3	-	High level requirement.
		NFM4	TC-NFM4	
		NFM5	TC-NFM5	
		NFM6	TC-NFM6	
		NFM7	TC-NFM7	
		NFM8	TC-NFM8	
		NFM9	TC-NFM9	
		NFM10	TC-NFM10	
7.2	Back-Off Trigger	BTR1	TC-BTR1	
		BTR2	TC-BTR2	
		BTR3	TC-BTR3	
		BTR4	TC-BTR4	
7.3	Back-Off Timer	BTI1	TC-NFM2	
		BTI2	TC-BTI2	
		BTI3	TC-BTI3	
		BTI4	TC-BTI4	
		BTI5	-	High level requirement.

IoT Device Connection Efficiency Guidelines Section		Requirement	Test Case	Comments
		BTI6	TC-NFM7	
		BTI7	TC-BTI7	
		BTI8	-	High level requirement.
		BTI9	TC-BTI9	
		BTI10	-	High level requirement.
		BTI11	-	High level requirement.
		BTI12	TC-BTI12	
7.5	IoT Device Action Linked to Cause Code	NER1	TC-NER1	
8.2.1	Radio Policy Manager - General	RPG1	TC-RPG1	
		RPG2	TC-RPG2	
		RPG3	TC-RPG3	
		RPG4	TC-RPG4	
		RPG5	TC-RPG5a TC-RPG5b TC-RPG5c	
		RPG6	TC-RPG6	
8.2.2	Radio Policy Manager - Mobility Management	RMM1	-	High level requirement.
		RMM2	TC-RMM2	
		RMM3	TC-RMM3a TC-RMM3b TC-RMM3c	
		RMM4	TC-RMM3a TC-RMM3b	
		RMM5	TC-RMM3a	
		RMM6	TC-RMM6a TC-RMM6b TC-RMM6c	
		RMM7	TC-RMM6a TC-RMM6b TC-RMM6c	
		RMM8	-	For future study
		RMM9	TC-RMM9	
		RMM10	TC-RMM10	
8.2.3	Radio Policy Manager – Session Management	RSM1	TC-RSM1	
		RSM2	TC-RSM1	
		RSM3	TC-RSM3	
		RSM4	TC-RSM3	
		RSM5	TC-RSM5	
		RSM6	TC-RSM5	
		RSM7	TC-RSM1 TC-RSM3 TC-RSM5	
		RSM8	TC-RSM8	
		RSM9	TC-RSM8	
8.2.4	Timers and Counters	RTC1	TC-RMM6a	

IoT Device Connection Efficiency Guidelines Section		Requirement	Test Case	Comments
			TC-RMM6b TC-RMM6c	
		RTC2	-	For future study
		RTC3	-	For future study
		RTC4	TC-RTC4	
		RTC5	TC-RTC4	
		RTC6	TC-RTC4	
		RTC7	TC-RTC7	
		RTC8	TC-RTC8	
		RTC9	TC-RPG5a TC-RPG5b TC-RPG5c	
		RTC10	TC-RPG1	
9.1	Rejection of IoT Device Requests with Back-off Timer	The requirements in section 9 of the guidelines document relates to features standardised by 3GPP. Please refer to the associated GCF or PTCRB test cases.		
9.2	Handling of Low Access Priority Indicator			
9.3	Implicit Reject in GSM Radio Network			
9.4	Long Periodic LAU/RAU/TAU			
9.5	Extended Access Barring			
9.6	Extended NMO-I			
9.7	Minimum Periodic Search Timer			
9.8	Attach with IMSI Indicator			
9.9	Timer T3245			
9.10	Configuration of 3GPP Release 10 Connection Efficiency Parameters			
9.11	Power Saving Mode			

5 Test Cases

5.1 IoT Device Application Test Cases

5.1.1 TC-DAR1

Purpose	To test the “Always-on” connectivity mechanism for an IoT Device Application that very frequently sends data.
Requirement under test	DAR1
Entry Criteria	1. IoT Device Application is capable to send frequent data.
Test Procedure	1. IoT Device registers to network and data connection is successfully established. 2. Observe the Radio Resource Control (RRC) state, RRC connection Setup and Release in the Network for certain interval.
Exit Criteria (Pass Criteria)	1. IoT Device shall not make frequent RRC connection Setup and Release requests and it should be in one of the RRC state machines depending on data payload.

5.1.2 TC-DAR2

Purpose	Test that the IoT Device Application “stores and forwards” data to minimise the number of network connections made by the device.
Requirement under test	DAR2
Entry Criteria	1. IoT Device Application is capable to store the data. 2. IoT Device shall have enough memory.
Test Procedure	1. IoT Device registers to the network and a data connection is successfully established. 2. Observe the data payload transferred over the network. 3. Observe the RRC state changes of the device via IoT Device logs or network logs.
Exit Criteria	1. IoT Device shall aggregate the user data such that there is not a 1:1 ratio between user data messages and RRC connection setup and release requests. 2. IoT Device shall send big chunks of user data payload wherever possible.

5.1.3 TC-DAR3

Purpose	Check that the IoT Device avoids IoT Device Application timing synchronization.
Requirement under test	DAR3
Entry Criteria	1. At least two IoT Devices are needed. 2. IoT Device Application shall be capable to send data on request or at regular intervals.
Test Procedure	1. IoT Device#1 registers to the network and a data connection is successfully established. 2. Wait for a random time interval of > 2 minutes. 3. IoT Device#2 registers to the network and a data connection is successfully established. 4. Steps 1 to 3 should repeated for each IoT Device involved in the test. 5. All of the IoT Devices shall send “keep-alive” messages/data/SMSs to the network. 6. Observe the IoT Device Applications and monitor the data payload for a certain interval. NOTE: If possible, keep the network timers to smaller values, so that test can be done in short period.
Exit Criteria	1. All of the IoT Devices shall send their network connection requests at randomized time intervals.

5.1.4 TC-DAR5

5.1.4.1 TC-DAR5a

Purpose	Check the device implements appropriate security measures to prevent unauthorized or insecure local device management.
Requirement under test	DAR5
Entry Criteria	1. IoT Device is capable of local device management.
Test Procedure	1. Use a laptop to connect to the IoT Device (e.g. via USB cable). 2. Log in to the IoT Device. 3. Instruct the IoT Device to execute some device management commands. (e.g. Change APN settings)
Exit Criteria	1. For local device management, the IoT Device shall implement an authentication and authorization process (for example, using username and password) to prevent unauthorized access to device management functionality.

5.1.4.2 TC-DAR5b

Purpose	Check the device implements appropriate security measures to prevent unauthorized or insecure remote device management.
Requirement under test	DAR5
Entry Criteria	1. The IoT Device is capable of remote device management. 2. The IoT Device can connect to a suitable configured remote device management platform.
Test Procedure	1. Connect the device to the network. 2. Let the IoT Device connect remote device management platform. 3. Let the remote device management platform send one or more device management commands to the IoT Device. **Note:** There are several ways to perform remote management of an IoT Device, such as OMA DM protocol, OMA LWM2M protocol, proprietary OTA mechanisms etc.
Exit Criteria	1. For remote device management, the IoT Device shall implement an authentication process of the remote device management platform when it connects to the platform.

5.1.5 TC-DAR6

Purpose	Check the IoT Device Application uses dynamic polling intervals.
Requirement under test	DAR6
Entry Criteria	1. IoT Device Application shall be capable to send the ‘Keep-alive’ message 2. TCP_IDLE value of the network shall be set to 30 minutes.

Test Procedure	1. IoT Device registers to the network and a data connection is successfully established. 2. Keep the IoT Device attached to the network and wait for a while (depends on Network settings (TCP_IDLE), but max 30 minutes). 3. Observe the keep-alive message and its interval.
Exit Criteria	1. IoT Device application shall adjust its polling interval to send the keep-alive message which is less than TCP_IDLE value or <30 minutes. Over this period IoT Device application polling interval shall be adjusted.

5.1.6 TC-DAR7

Purpose	Check if the IoT Device Application uses a fixed polling interval.
Requirement under test	DAR7
Entry Criteria	1. IoT Device application is capable to send the 'Keep-alive' message, but doesn't support dynamic polling interval.
Test Procedure	1. IoT Device registers to the network and a data connection is successfully established. 2. Keep the IoT Device attached to the network and wait for a while (max 30 minutes) 3. Observe the Keep-alive message and its interval.
Exit Criteria	1. IoT Device application sends the keep-alive message every 29 minutes. **Note:** The default value of 29 minutes is recommended because the routers used by many Mobile Network Operators' will clear the Network Address Translation (NAT) entry for the IoT Device's data session 30 minutes after the last communication is sent to/from the IoT Device.

5.1.7 TC-DAR8

Purpose	Check if the IoT Device Application adapts to changes in network communication latency and data speed.
Requirement under test	DAR8, DAR9.
Entry Criteria	1. IoT Device application is capable to send frequent data. 2. IoT Device shall support UMTS/HSPA. 3. IoT Device Application shall adapt its behaviour depending upon the network data speed and latency.
Test Procedure	1. Enable the UMTS/HSPA cell. 2. IoT Device registers to the network and a data connection is successfully established. 3. Enable the EUL/HS capability in the network. 4. Observe the RRC state changes and radio bearer used during the test. 5. Observe the behaviour of the IoT Device Application. 6. Downgrade the cell capability to 64/64 kbps DCH. 7. Observe the RRC state changes and radio bearer used during the test.

	8. Observe the behaviour of the IoT Device Application. 9. Increase the Latency delay in the Latency server. 10. Observe the behaviour of the IoT Device Application. 11. Revert to default value of Latency in the network latency server.
Exit Criteria	1. The IoT Device Application shall be adapt its behaviour to cope with variances in mobile network data speed and latency.

5.1.8 TC-DAR11

5.1.8.1 TC-DAR11a

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • SIM Subscription placed in a terminated state
Requirement under test	DAR11
Entry Criteria	1. SIM Subscription set as terminated (i.e. IoT Service not allowed permanently). 2. In this scenario the subscription must not exist in the HLR.
Test Procedure	1. Switch on the device and try to operate normally. 2. Observe that the data connection shall fail. 3. Observe the device behaviour for a period of time
Exit Criteria	1. The Device should not retry a service request and “back off” according to the functionality defined within ‘network friendly mode’ or ‘radio policy manager’.

5.1.8.2 TC-DAR11b

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • SIM Subscription with roaming not allowed
Requirement under test	DAR11
Entry Criteria	1. The subscription associated with the IoT Device exists in the HLR but service is temporarily not allowed.
Test Procedure	Two different situations can be verified: a. The change in service is carried out when the device is running, i.e. during its normal operation. b. The change in service has been done before the device is switched on. For case a): 1. Make sure the SIM subscription has its normal configuration with respect to communications. 2. Switch on the device and check that the PDP context is properly established. 3. Log into your HLR service platform and change the subscription

	configuration to “Roaming Not Allowed” 4. Try to operate normally. 5. Observe that the data connection shall fail. 6. Observe the device behaviour for a period of time For case b): 1. Make sure the HLR subscription has the subscription configuration “Roaming Not Allowed”. 2. Switch on the device and try to operate normally.
Exit Criteria	1. The IoT Device should not retry a service request and “back off” according to the functionality defined within ‘network friendly mode’ or ‘radio policy manager’.

5.1.8.3 TC-DAR11c

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • SIM Subscription with barred GPRS service
Requirement under test	DAR11
Entry Criteria	1. The SIM subscription associated with the IoT Device exists in the HLR and M2M Service is allowed but GPRS service is not allowed.
Test Procedure	Two different situations can be verified: a. The GPRS service is removed when the device is running, i.e. during its normal operation. b. The GPRS service is not allowed when the device is switched on. For case a): 1. Make sure the SIM subscription has its normal configuration with respect to communications. 2. Switch on the device and check that the PDP context is properly established. 3. Log into your HLR service platform and change the subscription configuration to “GPRS Not Allowed” 4. Try to operate normally. 5. Observe that the data connection shall fail. 6. Observe the device behaviour for a period of time For case b): 1. Make sure the HLR subscription has the subscription configuration “GPRS Not Allowed”. 2. Switch on the device and try to operate normally. 3. Observe that the data connection shall fail. 4. Observe the device behaviour for a period of time
Exit Criteria	1. The IoT Device should not retry a service request and “back off” according to the functionality defined within ‘network friendly mode’ or ‘radio policy manager’.

5.1.8.4 TC-DAR11d

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • Failure to set up a data connection due to wrong APN configuration
Requirement under test	DAR11
Entry Criteria	1. SIM subscription configuration is correct but the GGSN rejects the request. 2. Configure a wrong APN in the Device (a different APN from the one which provides the correct connectivity). 3. Observe that the data connection shall fail. 4. Observe the device behaviour for a period of time
Test Procedure	1. Operate the device normally and try to set up a data session.
Exit Criteria	1. The IoT Device should not retry a service request and “back off” according to the functionality defined within ‘network friendly mode’ or ‘radio policy manager’.

5.1.8.5 TC-DAR11e

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • Failure to set up a data connection due to Radius rejection
Requirement under test	DAR11
Entry Criteria	1. The SIM subscription configuration is correct 2. Radius authentication is configured and enabled in both the device and network 3. Observe that the data connection shall fail. 4. Observe the device behaviour for a period of time
Test Procedure	1. Change the ID or the password in the device, reset the connection and try to set up a data session.
Exit Criteria	1. The IoT Device should not retry a service request and “back off” according to the functionality defined within ‘network friendly mode’ or ‘radio policy manager’.

5.1.8.6 TC-DAR11f

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • IoT Service Platform is offline.
Requirement under test	DAR11
Entry Criteria	1. The IoT Device is properly configured (APN etc.). 2. SIM Subscription is active and is configured with the necessary services.

	3. The IP and port of the IoT Service Platform is reachable and no firewall is blocking them.
Test Procedure	1. Shut down the IoT Service Platform so that it is offline. 2. Switch on the device and check that the PDP context is properly established. 3. Try to set up a data session to the IoT Service Platform. 4. Observe that the data connection shall fail. 5. Observe the device behaviour for a period of time
Exit Criteria	1. The IoT Device should not retry the service request and “back off” according to the functionality defined within ‘network friendly mode’ or ‘radio policy manager’.

5.1.8.7 TC-DAR11g

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • IoT Service Platform’s IP address is unreachable.
Requirement under test	DAR11
Entry Criteria	1. The device is properly configured (APN etc.) 2. SIM Subscription is activate and is configured with the necessary services. 3. Block the IP address of the IoT Service Platform using by a firewall, or configure the device with an IP address (or port) which is not reachable.
Test Procedure	1. Connect the device to the network. 2. Operate the device normally and try to set up a data session. 3. Observe that the data connection shall fail. 4. Observe the device behaviour for a period of time.
Exit Criteria	1. The Device should not retry a service request and “back off” according to the functionality defined within ‘network friendly mode’ or ‘radio policy manager’.

5.1.8.8 TC-DAR11h

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • SMS Centre unreachable.
Requirement under test	DAR11
Entry Criteria	1. Configure a wrong SMSC in the device.
Test Procedure	1. Connect the device to the network. 2. Operate the device normally and try to send an SMS from the device. 3. Observe that the SMS shall fail. 4. Observe the device behaviour for a period of time.

Exit Criteria	1. The Device should not retry the SMS service request and “back off” according to the functionality defined within ‘network friendly mode’ or ‘radio policy manager’.

5.1.8.9 TC-DAR11i

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • Subscription with MO SMS barred.
Requirement under test	DAR11
Entry Criteria	1. Subscription configuration in the HLR shall be set to “SMS MO NOT ALLOWED”.
Test Procedure	1. Connect the device to the network. 2. Operate the device normally and try to send an SMS from the device. 3. Observe that the SMS shall fail. 4. Observe the device behaviour for a period of time.
Exit Criteria	1. The Device should not retry the SMS service request and “back off” according to the functionality defined within ‘network friendly mode’ or ‘radio policy manager’.

5.1.9 TC-DAR12

Purpose	Check IoT Device Application behaviour when the number of PDP context establishment attempts within a certain time period exceeds a defined value.
Requirement under test	DAR12
Entry Criteria	1. A maximum number of connection attempts for a specified period of time shall be set within the IoT Device. This information shall be known to the tester. 2. The IoT Device should be configured to perform back-off procedures after a specified number of connection attempts is exceed over a set period of time. This is set by IoT Service Platform.
Test Procedure	1. Switch on the IoT Device & it successfully registers to the network. 2. Configure the IoT Device with an invalid APN or set the network to ‘**reject’** the following request: a. PDP context activation 3. Send AT commands to initiate the PDP context or keep the device registered and let it try to initiate a PDP context (if IoT Device is capable to do) 4. Observe the device behaviour when the data connection limit is reached 5. Observe the device behaviour when the data connection time limit has expired.

Exit Criteria	1. IoT Device shall have a mechanism to set the data connection limit and time limit as defined by the IoT Service Platform 2. IoT Device or network traces/logs shall show that when the maximum number of connection attempts is reached the IoT Device shall stop attempting to connect to the network until after the defined time period expires. 3. The IoT Device shall inform the IoT Service Platform about the number of connection attempts.

5.1.10 TC-DAR13

Purpose	Check IoT Device Application behaviour when the data volume limit with a certain time period is exceeded.
Requirement under test	DAR13
Entry Criteria	1. A data volume limit for a specified period of time shall be set within the IoT Device. This information shall be known to the tester IoT Device application is capable to send frequent data. 2. The IoT Device should be configured to perform back-off procedures after a specified data limit is exceed over a set period of time. This is set by IoT Service Platform.
Test Procedure	1. Switch on the IoT Device so that it successfully establishes a PDP connection. 2. IoT Device initiates data transfer. 3. Observe the data payload and its connection activities in the network. 4. Observe the device behaviour when the data volume limit is reached 5. Observe the device behaviour when the data volume time limit has expired. NOTE: To minimize test time, define the data volume limit and period of time in the IoT Service Platform to a small value.
Exit Criteria	1. IoT Device shall have a mechanism to set the data volume limit and time limit as defined by the IoT Service Platform. 2. IoT Device or network traces/logs shall show that when the data volume exceeds that defined by IoT Service Platform the IoT Device should not initiate any further data transfer until the defined time period expires. 3. IoT Device should inform the IoT Service Platform about data volume used.

5.1.11 TC-DAR14

Purpose	Check IoT Device Application reports power failures.
Requirement under test	DAR14
Entry Criteria	IoT Device Application is capable to send a notification of power status to IoT Service Platform.
Test Procedure	Two different situations can be tested under following assumptions: a. Unexpected power outage is carried out when the device is running, i.e.

	during its normal operation. b. Unexpected battery power problem is carried out when the device is running For case a): 1. Power on the device 2. Device connects to the network 3. Wait until the IoT Device is connected to the IoT Service Platform. 4. Pull the power plug out of IoT Device. 5. Reconnect the power plug. 6. Power on the device 7. Device connects to the network 8. Check if there is a notification which has sent to IoT service platform For case b): 1. Replace the normal power supply of the IoT Device with a digital power supply. 2. Power on the device 3. Device connects to the network 4. Wait until the IoT Device is connected to the IoT Service Platform. 5. Set the voltage of power supply below the lower limit of IoT Device 6. Set the voltage of power supply back to the devices normal level 7. Check if there is a notification which has sent to IoT service platform.
Exit Criteria	1. IoT Device shall inform IoT service platform about power status.

5.1.12 TC-DAR16

Purpose	Check IoT Device Application's use of "off-peak' communication.
Requirement under test	DAR16
Entry Criteria	1. IoT Device Application is configured to send data to the IoT Service Platform at a specified time of day (i.e. during 'off peak' hours). 2. Ensure the time is correctly set within the device, network and IoT Service Platform.
Test Procedure	1. Connection between the IoT Device and IoT Service Platform is successfully established 2. Let IoT Device operate for a certain time period of time which includes "peak" hours and "off-peak" hours and allow it to send data to IoT Service Platform. 3. If necessary adjust the clock within the IoT Device to test 'peak' and 'off peak' behaviour. 4. Obtain network signalling logs or CDRs from the network.
Exit Criteria	1. Review network logs signalling or CDRs to ensure the application's network communication takes place during 'off peak' periods and that data connection activity is not concentrated during peak hours.

5.1.13 TC-DAR19

Purpose	Check behaviour of IoT Device Application when resetting the Communications Module after any communication failures or error conditions.
Requirement under test	DAR19
Entry Criteria	1. IoT Device's Communication Module supports Network Friendly Mode or Radio Policy Manager and this functionality is active.
Test Procedure	1. Connection between IoT Device and IoT Service Platform is successfully established 2. Repeatedly instruct the IoT Device Application to reboot of the Communication Module, or configure a scenario that is known to result in the IoT Application sending reboot commands to the Communications Module. 3. Observe the RRC state, RRC connection Setup and Release in the Network for certain interval
Exit Criteria	1. After a certain time period the Communications Module shall block requests from the IoT Device Application to restart the IoT Communication Module. 2. Network Friendly Mode or Radio Policy Manager behaviour by the Communications Module shall be observed.

5.1.14 TC-DAR20

Purpose	Check behaviour of IoT Device Application in Low power mode
Requirement under test	DAR20
Entry Criteria	1. IoT Device need to perform irregular data transmissions 2. IoT Device application shall tolerate some latency for its IoT Service
Test Procedure	1. Connection between IoT Device and IoT Service Platform is successfully established 2. Let IoT Device operate for some time 3. For IoT Device, observe device log or indicator light to see whether or not IoT Device is in a 'low power' mode for the time periods in-between sending data to the IoT Service Platform. 4. For IoT Device Communication Module, observe the RRC state changes
Exit Criteria	1. IoT Device enters into 'low power' mode for the time periods in-between sending data to the IoT Service Platform.

5.1.15 TC-DAR21

5.1.15.1 TC-DAR21a

Purpose	Check IoT Device Application uses a secure data connection.
Requirement	DAR21

under test	
Entry Criteria	1. IoT Service platform only allows the communication after authenticating the IoT Device. 2. IoT Service platform and IoT Device application communicates securely. 3. IoT Device shall be UMTS/HSPA capable.
Test Procedure	1. Enable the UMTS/HSPA cell with EUL/HS or DCH/DCH capability 2. IoT Device is registered to network and PS connection is successfully established towards network. 3. IoT Device establishes connection to the IoT Service Platform. 4. Observe the TCP/IP traces and its return packets for certain period.
Exit Criteria	1. IoT Service platform establishes SSL (Secured Socket Layer - 128/256 bit) connection with the IoT Device application and exchange encrypted data between them.

5.1.15.2 TC- DAR21b

Purpose	Check for certificate handshake when establishing a secure data connection
Requirement under test	DAR21
Entry Criteria	1. IoT Service platform only allows the communication after authenticating the IoT Device. 2. IoT Service platform and IoT Device application communicates securely. 3. IoT Device shall be UMTS/HSPA capable.
Test Procedure	*To be defined*
Exit Criteria	1. IoT Service platform establishes SSL (Secured Socket Layer - 128/256 bit) connection with the IoT Device application and exchange encrypted data between them.

5.1.16 TC-DAR22

5.1.16.1 TC-DAR22a

Purpose	Check IoT Device authentication (based on IMSI) towards IoT Service Platform.
Requirement under test	DAR22
Entry Criteria	1. IoT Service platform only allows the communication after authenticating the IoT Device 2. Two devices and 2 SIM cards are needed. Only one IMSI is provisioned in the IoT Service Platform. 3. IoT Device shall be UMTS/HSPA capable.
Test Procedure	1. Enable the UMTS/HSPA cell with EUL/HS or DCH/DCH capability 2. IoT Devices are registered to network. 3. Initiate PDP request from both the devices. 4. Trigger the data towards IoT Service Platform. 5. Observe the TCP/IP traces and its return packets for certain period

Exit Criteria	1. IoT Service platform shall only communicate with IoT Devices who's IMSIs are registered in the service platform.

5.1.16.2 TC-DAR22b

Purpose	Check IoT Device authentication (based on specific APN) towards IoT service platform.
Requirement under test	DAR22
Entry Criteria	IoT Service Platform only allows communication after authenticating the IoT Device by its APN. Two IoT Devices and 2 SIM cards are needed. Only device is configured with an APN which authenticates to the IoT Service Platform. IoT Device shall be UMTS/HSPA capable.
Test Procedure	1. Enable the UMTS/HSPA cell with EUL/HS or DCH/DCH capability. 2. IoT Devices are registered to network. 3. Initiate PDP request from both the devices. 4. Trigger the data towards IoT service platform / enterprise server. 5. Observe the TCP/IP traces and its return packets for certain period.
Exit Criteria	1. IoT Service platform shall only communicate with the IoT Device that has a valid APN.

5.1.17 TC-DAR24

Purpose	Check IoT Device and its Communication Module are "reset to factory settings".
Requirement under test	DAR24
Entry Criteria	1. IoT Device (and its Communication Module) can be reset to factory settings locally and remotely.
Test Procedure	1. For local reset: a. Use laptop to connect IoT Device. b. Issue a command to reset IoT Device (and Communication Module) to its factory settings. c. Reboot IoT Device. 2. Remote connection: a. IoT Device connects to IoT Service Platform. b. Reset IoT Device (and Communication Module) to its factory settings from the IoT Service Platform. c. Reboot IoT Device.
Exit Criteria	1. For both local and remote cases, after rebooting, check the IoT Device (and Communication Module) has been reset to its factory settings.

5.1.18 TC-DAR25

Purpose	Check IoT Device and its Communication Module supports "time

	resynchronisation" via remote and local connection.
Requirement under test	DAR25
Entry Criteria	1. IoT Device (and its Communication Module) supports "time resynchronisation" via local and remote connection. 2. Clock is incorrectly set in the IoT Device (and its Communication Module).
Test Procedure	1. For local reset: a. Use laptop to connect IoT Device. b. Check the clock in the IoT Device (and its Communication Module). c. Issue a command to resynchronise the clock in the IoT Device (and its Communication Module). d. Read the clock in the IoT Device (and its Communication Module). 2. Remote connection: a. IoT Device connects to IoT Service Platform. b. Check the clock in the IoT Device (and its Communication Module). c. Resynchronise the clock in the IoT Device (and Communication Module) by sending a command from the IoT Service Platform. d. Check the clock in the IoT Device (and its Communication Module).
Exit Criteria	1. For both local and remote cases, after issuing the time resynchronisation command, check the clock in the IoT Device (and Communication Module) is correctly set.

5.2 Communications Module Test Cases

5.2.1 IPv6 Test Cases

5.2.1.1 TC-IP1

Purpose	Check the IoT Communications Module does not send unsolicited messages
Requirement under test	IP1
Entry Criteria	1. IoT Device shall be configured to use IPv6 addressing. 2. Test network shall support IPv6 addressing. 3. APN should be only IPv6 capable
Test Procedure	1. Enable IoT Device and allow it to register to the network. 2. Monitor the IP traffic from the device using a traffic analyser.
Exit Criteria	1. Check that IoT Device does not send unsolicited IP messages.

5.2.1.2 TC-IP2

Purpose	Check the IoT Communications Module sends only a AAAA DNS Query.

Requirement under test	IP2
Entry Criteria	1. IoT Device shall be configured to use IPv6 addressing. 2. Test network shall support IPv6 addressing. 3. APN should be only IPv6 capable
Test Procedure	1. Enable IoT Device and allow it to register to the network. 2. Generate a DNS query from IoT Device. 3. Monitor the IP traffic from the device using a traffic analyser.
Exit Criteria	1. Check that the IoT Device generates only AAAA DNS query.

5.2.1.3 TC-IP3

Purpose	Check the Communications Module management system is IPv6 based
Requirement under test	IP3
Entry Criteria	1. IoT Device shall be configured to use IPv6 addressing. 2. Test network shall support IPv6 addressing.
Test Procedure	1. Enable IoT Device and allow it to register to the network. 2. Check that Stateless Address Auto-configuration (SLAAC) works properly within IoT Device. 3. Using PC with IPv6 enabled try to connect to the IoT Device’s management system.
Exit Criteria	1. Check that the Communications Module management system is IPv6 based.

5.2.1.4 TC-IP4

Purpose	Check the Communications Module shall supports, Neighbour Discovery, Stateless Address Auto Configuration, ICMPv6 protocol, IPv6 addressing architecture and IPv6 address text representation.
Requirement under test	IP4
Entry Criteria	1. IoT Device shall be configured to use IPv6 addressing. 2. Test network shall support IPv6 addressing. 3. APN should be only IPv6 capable.
Test Procedure	1. Enable IoT Device and allow it to register to the network. 2. Using traffic analyser check, that IoT Device generates Neighbour Discovery messages. 3. After registering in the network, check that SLAAC properly works in IoT Device. 4. Ping a known valid IPv6 host using standard IPv6 addressing and wait for a reply. 5. Ping a valid IPv6 host using IPv6 address text representation and wait for a reply.
Exit Criteria	1. IoT Device generates Neighbour Discovery messages

	2. SLAAC works properly 3. In case if the IoT Device receives responses to the pings ICMPv6 protocol works properly.

5.2.1.5 TC-IP5

Purpose	Check the Communications Module supports Privacy Extensions for Stateless Address Auto-configuration in IPv6, ROHC, Router Advertisement Flags Options and Path MTU discovery
Requirement under test	IP5
Entry Criteria	1. IoT Device shall be configured to use IPv6 addressing. 2. Test network shall support IPv6 addressing. 3. APN should be only IPv6 capable.
Test Procedure	1. Enable IoT Device and allow it to register to the network. 2. Auto-configuration of IPv6 addresses typically involves concatenating a prefix with an interface identifier. The prefix should be FE80::/10 for an auto-configured link-local address or a global prefix provided by a network. 3. Using traffic analyser check, that IoT Device is capable with Robust Header Compression. 4. Connect IoT Device to an IPv6 server. 5. Using traffic analyser check, that IoT Device performs Path MTU Discovery.
Exit Criteria	1. Check logs to ensure Device support auto-configuration of IPv6 addresses. 2. Check logs to ensure Device supports Robust Header Compression. 3. Check logs to ensure Device supports Path MTU Discovery.

5.2.2 Fast Dormancy Test Case

5.2.2.1 TC-CFD1 (Ed Note: T323 need to be mentioned in this test case)

Purpose	Triggering of the ‘Fast Dormancy algorithm’ within the Communications based on IoT Device data inactivity.
Requirement under test	CFD1
Entry Criteria	1. IoT Communication Module shall support either 3GPP Pre-Release 8 or 3GPP Release 8 Fast Dormancy features.
Test Procedure	1. Enable the UMTS/HSPA cell with EUL/HS or DCH/DCH capability with Fast dormancy enabled. 2. Keep the ‘down switch timer’ and ‘DCH timer’ to smaller value. 3. IoT Device is registered to network and the PDP request initiated from the device. 4. Initiate a data transfer from the IoT Device / device application. 5. Wait for one minute. 6. Pause the data transfer from the IoT Device / device application. 7. Observe the network races for the messages from IoT Communication

	Module. 8. Resume the data transfer from the IoT Device / device application. 9. Observe the network races for the messages from IoT Communication Module.
Exit criteria	1. For 3GPP Pre-Release 8 devices: Once the data transfer is stopped; IoT Communication Module's RRC state shall change from DCH to IDLE directly without 'any cause'. 2. For 3GPP Release 8 devices onwards: Once the data transfer is stopped, RRC state shall change from DCH to URA_PCH by sending Signalling connection Release indication with 'PS data session ends' cause. 3. Once the data is resumed; IoT Communication Module shall switch from URA_PCH/IDLE state to FACH by sending cell update and then to DCH (depending on data rate)

5.2.3 Security Test Cases

5.2.3.1 TC-MSR2

Purpose	To test that network connections and (U)SIM authenticated services are terminated when (U)SIM is removed from the Communications Module.
Requirement under test	MSR2
Entry Criteria	1. IoT Device has a (U)SIM inserted that is allowed to register on a network.
Test Procedure	1. Power on the IoT Device with the (U)SIM inserted. 2. Perform necessary actions to register the IoT Device on a network. 3. Verify that the IoT Device successfully registers to the network. 4. Remove (U)SIM from the IoT Device (ideally without powering down the device). 5. Verify that the IoT Device is no longer registered on the network. 6. Without re-inserting the (U)SIM, perform necessary actions to register the IoT Device onto the network. 7. Verify the IoT Device is still able to register (emergency camp) to the network.
Exit criteria	1. Device shall immediately disconnect from the network when the (U)SIM is removed. 2. Device shall emergency camp to the network after the (U)SIM is removed.

5.2.3.2 TC-MSR4

Purpose	To test that it is possible to lock the Communications Module to a unique (U)SIM.
Requirement under test	MSR4
Entry Criteria	1. The Communications Module has a (U)SIM inserted. 2. The Communications Module shall be locked (to the full IMSI) of the inserted (U)SIM.

Test Procedure	1. Power on the IoT Device with the (U)SIM inserted. 2. Perform necessary actions to register the IoT Device on a network. 3. Verify that the IoT Device successfully registers to the network. 4. Remove the (U)SIM and insert another (U)SIM with different IMSI. 5. Verify that the IoT Device rejects the (U)SIM and does not register to the network. 6. Perform necessary actions to remove the SIM lock from the IoT Device. 7. Perform necessary actions to register the IoT Device on a network. 8. Verify that the IoT Device now successfully registers to the network.
Exit criteria	1. The Communications Module shall refuse to register to the network using the 2nd (U)SIM until the SIM lock function is disabled

5.2.4 Subscription Identifier Test Cases

5.2.4.1 TC-IR1

Purpose	Check whether the Communications Module can support 15 digit Directory Numbers/MSISDNs.
Requirement under test	IR1
Entry Criteria	1. The IoT Device is able to access the cell network.
Test Procedure	1. Power on the IoT Device. 2. Start a Call from the IoT Device with a 15 digit MSISDN. 3. Observe the call setup message.
Exit Criteria (Pass Criteria)	1. In the call setup message, the MSISDN is same as the 15 digit MSISDN in step 2.

5.2.4.2 TC-IR2

Purpose	Check whether the Communications Module can support 2 and 3 digit based Mobile Network Codes IMSIs.
Requirement under test	IR2
Entry Criteria	1. The IoT Device is power off. A (U)SIM card with 15 digit IMSI (with 3 digit Mobile network code) is used in the IoT Device.
Test Procedure	1. Power on the IoT Device. 2. Wait for the location update request. 3. Observe the location update request. 4. Query the MCC and MNC from the device (e.g. using an AT command).
Exit Criteria (Pass Criteria)	1. In the location update request, the IMSI is 15 digit including 3 digit Mobile Network Code same as that in (U)SIM card. 2. Check that the device reports the correct 3 digit MNC in response to the query.

5.3 Connection Efficiency Test Cases

5.3.1 TC-NFM1

Purpose	Enable or Disable Network Friendly Mode feature.
Requirement under test	NFM1
Entry Criteria	1. IoT communication module supports NFM feature.
Test Procedure	1. Switch ON the IoT Device. 2. Send AT command to enable/disable NFM (e.g. AT+NFM=1[0,1] or AT+NFM=0).
Exit criteria	1. IoT communication module shall enable/disable NFM.

5.3.2 TC-NFM2

Purpose	Check IoT Device reports the value for the <NFM Active> and <Start Timer>using an AT command.
Requirement under test	NFM2, BTI1
Entry Criteria	1. IoT communication module supports NFM feature.
Test Procedure	1. Switch ON the IoT Device. 2. Send AT Command to read the status of NFM (e.g. AT+NFM=?).
Exit Criteria	1. IoT communication module shall return the value of <NFM Active> and <Start Timer>.

5.3.3 TC-NFM4

Purpose	Configuration of Back-off base interval.
Requirement under test	NFM4
Entry Criteria	1. IoT communication module supports NFM feature.
Test Procedure	1. Switch ON the device. 2. Set the Back-off base interval using e.g. AT+NFMC=60,120,240,480,960,1920,3840.
Exit Criteria	1. IoT communication module shall set the Back-off base interval.

5.3.4 TC-NFM5

Purpose	Read ‘Back-off timer array’ or ’Back-off timer flag’.
Requirement under test	NFM5
Entry Criteria	1. IoT communication module supports NFM feature.

Test Procedure	1. Switch ON the device. 2. Send AT command to enable the NFM feature. 3. Set the Back-off base interval using e.g. AT+NFMC=60,120,240,480,960,1920,3840. 4. Send AT command to read the 'back-off timer array' / 'back-off timer flag'.
Exit Criteria	1. IoT communication module shall return back-off status along with GSM Registration, GPRS registration, PDP and SMS back-off timers. e.g. Back-off Enabled: [0,1] Back-off Timer Active: [0,1] StartTimer: [0,1] Intervals: 60,120,240,480,960,1920,3840

5.3.5 TC-NFM6

Purpose	Verify whether the Communication Module rejects the IoT Device Application's request when the back-off timer is running.
Requirement under test	NFM6
Entry Criteria	1. IoT Communication Module supports NFM feature.
Test Procedure	1. Switch ON the IoT Device. 2. Send AT command to enable the NFM feature. 3. Configure the IoT Device or set the Network / Core Network to '**reject'** the one of the following requests: a. IMSI attach (e.g. an unsubscribe SIM can be used to create MM error 2, IoT Device need to configure to NOT do combined GRPS/IMSI attach). b. GPRS attach (NMO-II) (e.g. an unsubscribe SIM can be used to create GMM error 7, IoT Device needs to configure to do combined GRPS/IMSI attach). c. PDP context activation (e.g. the IoT Device can be configured with an invalid APN to create SM error 33). d. MO SMS (e.g. the IoT Device can be configure with an invalid SMS Service Centre to create RP error code 38). 4. Send AT command to read the back-off timer array. 5. Send another AT command to reinitiate the one of the above requests, while the previous back-off timer still has time remaining. 6. Observe the network traces or IoT Device trace/logs.
Exit Criteria	1. IoT Communication Module shall activate the back-off procedure once the request is rejected from the Network. 2. IoT Device shall display the back-off timer array. 3. IoT Communication Module shall ignore the new request while back-off countdown is active. 4. Network or Device traces and logs should reflect results.

5.3.6 TC-NFM7

Purpose	Restart the Back-off countdown again after power cycle.
Requirement under test	NFM7, BTI6
Entry Criteria	1. IoT communication module supports NFM feature.
Test Procedure	1. Switch ON the device 2. Send AT command to enable the NFM feature. 3. Configure the IoT Device or set the Network / Core Network to '**reject'** the one of the following requests. a. IMSI attach (e.g. an unsubscribe SIM can be used to create MM error 2, IoT Device need to configure to NOT do combined GRPS/IMSI attach). b. GPRS attach (NMO-II) (e.g. an unsubscribe SIM can be used to create GMM error 7, IoT Device needs to configure to do combined GRPS/IMSI attach). c. PDP context activation (e.g. the IoT Device can be configured with an invalid APN to create SM error 33). d. MO SMS (e.g. the IoT Device can be configure with an invalid SMS Service Centre to create RP error code 38). 4. Send AT command to read the back-off timer array. 5. Power cycle the IoT Device. 6. Send AT command to read the back-off timer array. 7. Send another AT command to reinitiate the one of the above requests. 8. Observe the network traces or IoT Device traces/logs.
Exit Criteria	1. IoT communication module shall activate the back-off procedure once the request is rejected from the Network. 2. IoT Device shall display the back-off timer array. 3. After power cycle the countdown timer shall be restarted and back-off shall be active. 4. IoT communication shall ignore the all new request while back-off countdown is active. 5. Network traces or Device traces/logs shall reflect results.

5.3.7 TC-NFM8

Purpose	Check IoT Device reports the supported range of values for parameters <NFM Active> and <Start Timer> using an AT command.
Requirement under test	NFM8
Entry Criteria	1. IoT communication module supports NFM feature.
Test Procedure	1. Switch ON the IoT Device. 2. Send AT Command to read the status of NFM (e.g. AT+NFM=?).
Exit Criteria	1. IoT communication module shall report the supported range of values for

	parameters <NFM Active> and <Start Timer>.

5.3.8 TC-NFM9

Purpose	Check IoT Device reports the value for the Back-off Base Interval using an AT command.
Requirement under test	NFM9
Entry Criteria	1. IoT communication module supports NFM feature.
Test Procedure	1. Switch ON the IoT Device. 2. Send AT Command to read the status of Back-off Base Interval (e.g. AT+NFMC?).
Exit Criteria	2. IoT communication module shall return the value of the Back-off Base Interval.

5.3.9 TC-NFM10

Purpose	Check IoT Device reports the supported range of values for the Back-off Base Interval using an AT command.
Requirement under test	NFM10
Entry Criteria	1. IoT communication module supports NFM feature.
Test Procedure	1. Switch ON the IoT Device. 2. Send AT Command to read the status of NFM (e.g. AT+NFMC=?).
Exit Criteria	1. IoT Communication Module shall return supported range of values for the Back-Off Base Interval.

5.3.10 TC-BTR1

Purpose	Back-off trigger for ‘IMSI attach failure’.
Requirement under test	BTR1
Entry Criteria	1. IoT communication module supports NFM feature.
Test Procedure	1. Switch ON the device. 2. Send AT command to enable the NFM feature. 3. Configure the IoT Device or set the Network / Core Network to ‘reject’ the following request. 4. IMSI attach (e.g. an unsubscribe SIM can be used to create MM error 2, IoT Device need to configure to NOT do combined GRPS/IMSI attach). 5. Send AT command to read the back-off timer array or back-off timer flag (whichever is implemented).
Exit Criteria	1. IoT communication module shall activate the back-off procedure once the request is rejected from the Network. 2. IoT Device shall display the 'GSM back-off timer array' and / or status of

	'back-off timer flag'.

5.3.11 TC-BTR2

Purpose	Back-off trigger for 'combined attach failure'.
Requirement under test	BTR2
Entry Criteria	1. IoT communication module supports NFM feature.
Test Procedure	1. Switch ON the device. 2. Send AT command to enable the NFM feature. 3. Configure the IoT Device or set the Network / Core Network to 'reject' the following request. 4. Combined attach (e.g. an unsubscribe SIM can be used to create GMM error 7, IoT Device needs to configure to do combined GRPS/IMSI attach). 5. Send AT command to read the back-off timer array or back-off timer flag (whichever is implemented).
Exit Criteria	1. IoT communication module shall activate the back-off procedure once the request is rejected from the Network. 2. IoT Device shall display the 'GSM and GPRS back-off timer array' and / or status of 'back-off timer flag'.

5.3.12 TC-BTR3

Purpose	Back-off trigger for 'PDP activation failure'.
Requirement under test	BTR3
Entry Criteria	1. IoT communication module supports NFM feature.
Test Procedure	1. Switch ON the device. 2. Send AT command to enable the NFM feature. 3. Configure the IoT Device or set the Network / Core Network to 'reject' the following request: 4. PDP activation request (e.g. the IoT Device can be configured with an invalid APN to create SM error 33). 5. Send AT command to read the back-off timer array or back-off timer flag (whichever is implemented).
Exit Criteria	1. IoT communication module shall activate the back-off procedure once the request is rejected from the Network. 2. IoT Device shall display the 'PDP back-off timer array' and / or status of 'back-off timer flag'.

5.3.13 TC-BTR4

Purpose	Back-off trigger for 'SMS failure'.
Requirement	BTR4

under test	
Entry Criteria	1. IoT communication module supports NFM feature.
Test Procedure	1. Switch ON the device. 2. Send AT command to enable the NFM feature. 3. Configure the IoT Device or set the Network / Core Network to ‘reject’ the following request. 4. MO SMS request (e.g. the IoT Device can be configured with an invalid SMS Service centre to create RP error code 38). 5. Send AT command to read the back-off timer array or back-off timer flag (whichever is implemented).
Exit Criteria	1. IoT communication module shall activate the back-off procedure once the request is rejected from the Network. 2. IoT Device shall display the ‘SMS back-off timer array' and / or the status of 'back-off timer flag'.

5.3.14 TC-BTI2

Purpose	Network Friendly Mode persistence after power cycle.
Requirement under test	BTI2
Entry Criteria	1. IoT communication module supports NFM feature.
Test Procedure	1. Switch ON the IoT Device. 2. Send AT command to activate the NFM (e.g. AT+NFM=1). 3. Send AT command to read NFM status. 4. Power cycle the IoT Device. 5. Send AT command to read NFM status.
Exit Criteria	1. IoT communication module shall return NFM Active (e.g. +NFM: [1,1]) before and after power cycle.

5.3.15 TC-BTI3

Purpose	Back-off timer flag status while timer is deactivated, then activated.
Requirement under test	BTI3
Entry Criteria	1. IoT communication module supports NFM feature.
Test Procedure	1. Switch ON the device. 2. Send AT command to enable the NFM feature. 3. Send AT command to read the ‘back-off timer array’ / ‘back-off flag’ status. 4. Configure the IoT Device or set the Network / Core Network to ‘reject’ the one of the following requests: a. IMSI attach (e.g. an unsubscribe SIM can be used to create MM error 2, IoT Device need to configure to NOT do combined GRPS/IMSI attach).

	b. GPRS attach (NMO-II) (e.g. an unsubscribe SIM can be used to create GMM error 7, IoT Device needs to configure to do combined GRPS/IMSI attach). c. PDP context activation (e.g. the IoT Device can be configured with an invalid APN to create SM error 33). d. MO SMS (e.g. the IoT Device can be configured with an invalid SMS Service Centre to create RP error code 38). 5. Send AT command to read the 'back-off timer array' / 'back-off flag' status.
Exit Criteria	1. IoT communication module shall return the 'back-off timer array' / 'back-off flag' status as deactivated. After NW error code; IoT communication module shall return the 'back-off timer array' / 'back-off flag' status as activated.

5.3.16 TC-BTI4

Purpose	Back-off timer flag persistence after power cycle
Requirement under test	BTI4
Entry Criteria	1. IoT communication module supports NFM feature
Test Procedure	1. Switch ON the IoT Device. 2. Send AT command to read the 'back-off timer array' / 'back-off flag' status. 3. Configure the IoT Device or set the Network / Core Network to 'reject' the one of the following requests: a. IMSI attach (e.g. an unsubscribe SIM can be used to create MM error 2, IoT Device need to configure to NOT do combined GRPS/IMSI attach). b. GPRS attach (NMO-II) (e.g. an unsubscribe SIM can be used to create GMM error 7, IoT Device needs to configure to do combined GRPS/IMSI attach). c. PDP context activation (e.g. the IoT Device can be configured with an invalid APN to create SM error 33). d. MO SMS (e.g. the IoT Device can be configured with an invalid SMS Service Centre to create RP error code 38). 4. Send AT command to read the 'back-off timer array' / 'back-off flag' status. 5. Once the back-off countdown started and before it elapses, Power cycle the IoT Device. 6. Send AT command to read the 'back-off timer array' / 'back-off flag' status.
Exit Criteria	1. IoT communication module shall return the 'back-off timer array' / 'back-off flag' status as deactivated. 2. After NW error code; IoT communication module shall return the 'back-off timer array' / 'back-off flag' status as activated.

	3. After power cycle; IoT communication module shall return the ‘back-off timer array’ / ‘back-off flag’ status as activated.

5.3.17 TC-BTI7

Purpose	Back-off Timer shall be reset and the Back-off Iteration Counter shall be reset after successful reattempt
Requirement under test	BTI7
Entry Criteria	1. IoT communication module supports NFM feature
Test Procedure	1. Switch ON the device. 2. Send AT command to enable the NFM feature (e.g. AT+MSOSTATUS=1). 3. Configure the IoT Device or set the Network / Core Network to ‘**reject’** the one of the following requests: a. GPRS attach (NMO-II) (e.g. an unsubscribe SIM can be used to create GMM error 7, IoT Device needs to configure to do combined GRPS/IMSI attach). b. PDP context activation (e.g. the IoT Device can be configured with an invalid APN to create SM error 33). c. MO SMS (e.g. the IoT Device can be configure with an invalid SMS Service Centre to create RP error code 38). 4. Send AT command to read the back-off timer array (e.g. AT+MSORETRYINFO?). 5. Set the Network / Core Network to ‘**accept**’ the above requests. 6. Wait for the Back-off timer to elapse. 7. Send another AT command to reinitiate the one of the above requests. 8. Send AT command to read the back-off timer array. 9. Observe the network traces or IoT Device traces/logs.
Exit Criteria	1. After NW error code; IoT communication module shall return the ‘back-off timer array’ status, the counter should show one error has occurred. 2. Back-off timer shall elapse. 3. After ‘accepted’ request; IoT communication module shall return the ‘back-off timer array’ / ‘back-off flag’ status as deactivated, the counter should be reset. 4. Network or Device traces/logs shall reflect results

5.3.18 TC-BTI9

Purpose	Test Randomization of back off timers.
Requirement under test	BTI9
Entry Criteria	1. IoT communication module supports NFM feature
Test Procedure	1. Switch ON the device 2. Send AT command to enable the NFM feature

	3. Send AT command to read the ‘back-off timer array’ / ‘back-off flag’ status 4. Configure the IoT Device or set the Network / Core Network to ‘reject’ the one of the following requests: a. IMSI attach (e.g. an unsubscribe SIM can be used to create MM error 2, IoT Device need to configure to NOT do combined GRPS/IMSI attach) b. GPRS attach (NMO-II) (e.g. an unsubscribe SIM can be used to create GMM error 7, IoT Device needs to configure to do combined GRPS/IMSI attach) 5. Send AT command to read the ‘back-off timer array’ / ‘back-off flag’ status
Exit Criteria	1. IoT communication module shall list the array/vector which contains GSM Registration, GPRS registration, PDP and SMS back-off timers and the countdown timer is different for different IoT Devices or different test of the same device. e.g. For Device 1: • GSM: 0,0,0,65 • GPR:1,0,0,147 • PDP: 2,0,0,0 • SMS: 3,0,0,0 For Device 2: • GSM: 0,0,0,72 • GPR:1,0,0,182 • PDP: 2,0,0,0 • SMS: 3,0,0,0

5.3.19 TC-BTI12

Purpose	Reset ‘Back-off timer array’ or ‘Back-off timer flag’.
Requirement under test	BTI12
Entry Criteria	1. IoT communication module supports NFM feature.
Test Procedure	1. Switch ON the device. 2. Get IoT Device to be in the back off state. 3. Send AT command to read the ‘back-off timer array’ and ‘Back-off timer flag’. 4. Send AT command to disable the ‘Back-off timer flag’. 5. Send AT command to read the ‘back-off timer array’ and ‘Back-off timer flag’.
Exit Criteria	1. When IoT Device is in the back-off state; the IoT communication module shall return the ‘back-off timer array’ / ‘back-off flag’ status as activated, with the timer’s number > 0. 2. After AT Command to disable ‘back-off timer flag’; IoT communication module shall return the ‘back-off timer array’ / ‘back-off flag’ status as deactivated, and the timer should be posted as 0.

5.3.20 TC-NER1

Purpose	Back-off trigger for network error codes.
Requirement under test	NER1
Entry Criteria	1. IoT communication module supports NFM feature.
Test Procedure	1. Switch ON the device. 2. Send AT command to enable the NFM feature. 3. Configure the IoT Device or set the Network / Core Network to ‘reject’ the IoT communication module with one of the error codes listed in the Section 7.5 [1]. 4. Send AT command to read the back-off timer array or back-off timer flag.
Exit Criteria	1. IoT Communication Module shall activate the back-off procedure (if applicable) once the request is rejected from the network.

5.4 Radio Policy Manager Test Cases

Please note that all the test cases under Radio policy management have entry criteria that IoT Device should be OFF before starting the test.

5.4.1 TC-RPG1

Purpose	Default RPM Parameters are stored on Chipset when (U)SIM does not have RPM Parameters.
Requirement under test	RPG1, RTC10
Entry Criteria	1. IoT Device application supports RPM features. 2. (U)SIM does not contain RPM parameters.
(U)SIM Parameter Settings	(U)SIM-RPM04 (See annex A)
Test Procedure	1. Power ON IoT Device. 2. Send Proprietary AT command to read RPM Parameters.
Exit Criteria	1. Make sure that RPM parameters matches with requirement RTC10.

5.4.2 TC-RPG2

Purpose	RPM Activation Control - RPM Parameters are present on (U)SIM.
Requirement under test	RPG2
Entry Criteria	1. IoT communication module supports RPM feature. 2. RPM parameters are present on (U)SIM and are different from the default values defined in requirement RTC10.
(U)SIM Parameter Settings	(U)SIM-RPM01 (See annex A)
Test Procedure	1. Read (U)SIM with Card Reader and record the RPM parameter settings. 2. Insert the (U)SIM into the device.

	3. Power ON IoT Device. 4. Send Proprietary AT command to read RPM parameters from the device.
Exit Criteria	1. Verify that following RPM parameters are reported by the device: a. DF-ARMED AGENT - 3F00/7F66/5F40 b. EF-RPM Enabled Flag - 3F00/7F66/5F40/4F40 c. EF-RPM Parameters - 3F00/7F66/5F40/4F41 d. EF-RPM Operational Management Counters Leak Rate – e. 3F00/ 7F66/5F40/ f. EF-RPM Operational Management Counters - 3F00/7F66/5F40/4F43 g. EF-RPM Version Information 3F00/7F66/5F40/4F44 2. Verify that the RPM parameters reported by the device match the values stored in the (U)SIM. 3. Verify the RPM functionality is enabled or disabled based on the setting of the parameter “RPM Enabled Flag” present on the (U)SIM.

5.4.3 TC-RPG3

Purpose	RPM Activation Control – When RPM Parameters are Not Present in (U)SIM
Requirement under test	RPG3
Entry Criteria	1. IoT Device application supports RPM features. 2. RPM parameters are not present in (U)SIM.
(U)SIM Parameter Settings	(U)SIM-RPM04 (See annex A)
Test Procedure	1. Power ON the IoT Device. 2. Send Proprietary AT command to read RPM Parameters “RPM Enabled Flag”.
Exit Criteria	1. RPM functionality shall be enabled or disabled based on the default setting of the parameter “RPM Enabled Flag” saved on the device.

5.4.4 TC-RPG4

Purpose	RPM is enabled when IoT Device is roaming.
Requirement under test	RPG4
Entry Criteria	1. IoT communication module supports RPM feature. 2. RPM parameters are present on SIM card. RPM_Enabled_Flag = ON.
(U)SIM Parameter Settings	(U)SIM-RPM01 (See annex A)
Test Procedure	1. Enable a Cell which is not the Home PLMN cell. 2. Power ON IoT Device and wait for it to perform a combined GPRS Attach. 3. Reject the GPRS Attach with GMM #6 (Illegal ME). 4. Verify IoT Device does not send GPRS Attach Request before T1 (+/-15%) after step 3.

	5. Verify IoT Device resets after time T1 (+/-15%) expires and attempts a combined GPRS Attach. 6. Reject the GPRS Attach with GMM #6 (Illegal ME). 7. Verify IoT Device does not send GPRS Attach Request before T1 (+/-15%) after step 6. 8. Verify IoT Device resets after time T1 (+/-15%) expires and attempts a combined GPRS Attach. 9. Accept GPRS Attach. 10. Verify RPM increments counter C-R-1 by 2. 11. Power OFF IoT Device and deactivate the cell.
Exit Criteria	1. Verify RPM is enabled and functionality is working in roaming network.

5.4.5 TC_RPG5

5.4.5.1 TC-RPG5a

Purpose	RPM can be disabled through SIM OTA.
Requirement under test	RPG5, RTC9
Entry Criteria	1. IoT communication module supports RPM feature. 2. RPM parameters are present on (U)SIM card. RPM_Enabled_Flag = ON.
(U)SIM Parameter Settings	(U)SIM-RPM01 (See annex A)
Test Procedure	1. Enable Cell on Network. 2. Power On IoT Device. 3. UE successfully registers on Network. 4. Send an OTA message with the configuration. Updates [USIM] ""RPM Enabled Flag"" file: [1] = 0 (disable)". 5. Confirm that the SMS message is correctly accepted and acknowledged. OTA shall not trigger registration from IoT Device. 6. Power cycle IoT Device, Wait for registration request from IoT Device. 7. This time Reject the Location Update Request with MM# 2 (IMSI UNKNOWN IN HLR). 8. Reject the GPRS Attach Request with GMM# 7 (GPRS SERVICES NOT ALLOWED). 9. Power off IoT Device.
Exit Criteria	1. Verify IoT Device does not attempt registration in the next 2 * T1 minutes after step 8.

5.4.5.2 TC-RPG5b

Purpose	A single RPM requirement can be disabled through SIM OTA.
Requirement under test	RPG5, RTC9, RMM8
Entry Criteria	1. IoT communication module supports RPM feature

	2. RPM parameters are present on (U)SIM card. RPM_Enabled_Flag = ON
(U)SIM Parameter Settings	(U)SIM-RPM01 (See annex A)
Test Procedure	1. Enable cell on Network. 2. Power ON IoT Device. 3. UE successfully registers on Network. 4. Send an OTA message with configuration Updates [USIM] ""RPM Parameters"" file [2] = 0 (set T1 to 0 to disable the requirement related to T1)". 5. Confirm that the SMS message is correctly accepted and acknowledged. OTA shall not trigger registration from IoT Device. 6. Power cycle IoT Device, Wait for registration request from IoT Device. 7. Reject the Location Update Request with MM# 2 (IMSI UNKNOWN IN HLR). 8. Reject the GPRS Attach Request with GMM# 7 (GPRS SERVICES NOT ALLOWED). 9. Wait for 2*T1. 10. Power off IoT Device.
Exit Criteria	1. Verify that IoT Device does not attempt registration during time in step 9.

5.4.5.3 TC-RPG5c

Purpose	Verify RPM is disabled when RPM_Enabled_Flag is OFF on (U)SIM card.
Requirement under test	RPG5, RTC9
Entry Criteria	1. IoT communication module supports RPM feature. 2. RPM parameters are present on (U)SIM card. RPM_Enabled_Flag = ON.
(U)SIM Parameter Settings	(U)SIM-RPM03 (See annex A)
Test Procedure	1. Switch ON the IoT Device. 2. Verify RPM is enabled. 3. Set RPM_Enabled_Flag to OFF on SIM card. 4. Verify RPM is disabled.
Exit Criteria	1. Verify RPM is enabled / disabled on the device as per the (U)SIM flag.

5.4.6 TC-RPG6

Purpose	Verify "RPM Version Implemented" file on (U)SIM card is updated with the correct RPM version.
Requirement under test	RPG6
Entry Criteria	1. IoT Device application supports RPM features. 2. RPM parameters are present on (U)SIM card: a. RPM_Enabled_Flag = ON.

	b. Parameter “EF-RPM Version Implemented” shall be set to = “00”.
(U)SIM Parameter Settings	(U)SIM-RPM01 (See annex A)
Test Procedure	1. Activate the cell. 2. Power ON IoT Device. 3. Accept Location Update Request and GPRS Attach Request. 4. Wait for 5 minutes. 5. Read "RPM Version Implemented" file on (U)SIM card. 6. Read "RPM Version Implemented" file through proprietary AT Command from device. 7. Power OFF IoT Device.
Exit Criteria	1. Verify that RPM Version is same in step 5 and 6.

5.4.7 TC-RMM2

Purpose	Verify that RPM operation management counters are reset after RPM parameters are updated through OTA.
Requirement under test	RMM2
Entry Criteria	1. IOT DEVICE is powered off. RPM parameters are present on SIM card. RPM_Enabled_Flag = ON
(U)SIM Parameter Settings	(U)SIM-RPM06 (See annex A)
Test Procedure	1. Enable a cell on Network 2. Power ON IoT Device. 3. IoT Device performs Location Update and GPRS attach successfully. 4. Send an OTA message with configuration: Updates [USIM] ""EF-RPM Operational Management Counters Leak Rate"" file: a. LR-1 = 24, b. LR-2 = 24, c. LR-3 = 24" 5. Confirm that the SMS message is correctly accepted and acknowledged. OTA shall not trigger registration from IoT Device. 6. Power off the IoT Device
Exit Criteria	1. Verify all counters in file "EF-RPM Operational management Counters" are reset to 0.

5.4.8 TC-RMM3

5.4.8.1 TC-RMM3a

Purpose	RPM controls number of SW resets when LU/Attach is rejected with permanent MM/GMM cause.
Requirement under test	RMM3, RMM4, RMM5
Entry Criteria	1. IoT communication module supports RPM feature.

(U)SIM Parameter Settings	(U)SIM-RPM02 (See annex A)
Test Procedure	1. Power up IoT Device. 2. Reject Location Update (LU) with MM# 3 (ILLEGAL MS); Reject GPRS Attach with GMM #7 (No PS services allowed). 3. SS uses AT command to reset IoT Device 2xN1 times in a period of one hour (evenly spaced). SS rejects each registration attempt with the same reject causes as in step 2. 4. Wait for 15 minutes. 5. SS uses AT command to reset IoT Device.
Exit Criteria	1. Verify SS only receives N1 registration attempts in step 3. 2. Verify RPM increments counter C-BR-1 by N1. 3. Verify registration is triggered for the reset in step 5.

5.4.8.2 TC-RMM3b

Purpose	RPM controls number of SW resets when Attach is rejected with permanent EMM cause.
Requirement under test	RMM3, RMM4
Entry Criteria	1. IoT Device application supports RPM features.
(U)SIM Parameter Settings	(U)SIM-RPM02 (See annex A)
Test Procedure	1. Power ON IoT Device. 2. Reject Attach Request with EMM cause #8 (EPS services and non-EPS services not allowed). 3. SS uses AT command to reset IoT Device 2xN1 times in a period of one hour (evenly spaced). SS rejects each Attach Request with EMM cause #8.
Exit Criteria	1. Verify SS only receives N1 Attach Requests in step 3.

5.4.8.3 TC-RMM3c

Purpose	Verify that RPM does not control the number of SW resets when N1 is set to 0.
Requirement under test	RMM3
Entry Criteria	1. IoT Device application supports RPM features.
(U)SIM Parameter Settings	(U)SIM-RPM11 (See annex A)
Test Procedure	1. Power ON IoT Device. 2. Reject Attach Request with MM cause #3 (Illegal MS). 3. SS uses AT command to reset IoT Device 12 times in a period of one hour (evenly spaced). SS rejects each Attach Request with MM cause #3.

Exit Criteria	1. Verify SS only receives 12 Attach Requests in step 3. 2. Verify C-BR-1 and C-R-1 are unchanged

5.4.9 TC-RMM6

5.4.9.1 TC-RMM6a

Purpose	RPM waits for time T1 and resets the modem after permanent MM/GMM reject.
Requirement under test	RMM6, RMM7, RTC1
Entry Criteria	1. IoT communication module supports RPM feature
(U)SIM Parameter Settings	(U)SIM-RPM01 (See annex A)
Test Procedure	1. Power on IoT Device. 2. Wait for ‘Location Update Request’ from IoT Device/ IoT communication module. 3. Reject the Location Update Request with MM# 2 (IMSI UNKNOWN IN HLR). 4. If IoT Device attempts GPRS Attach, Reject it with GMM #7 (No PS services allowed). 5. Accept Location Update Request and GPRS Attach Request. 6. Power OFF IoT Device.
Exit Criteria	1. Verify IoT Device does not send LU/Attach before T1 (+/-15%) after step 4. 2. Verify IoT Device attempts LU/Attach after T1 (+/-15%) expires. 3. Verify RPM increments counter C-R-1 by 1.

5.4.9.2 TC-RMM6b

Purpose	RPM waits for time T1 and resets the modem after permanent GMM reject.
Requirement under test	RMM6, RMM7, RTC1
Entry Criteria	1. IoT communication module supports RPM feature.
(U)SIM Parameter Settings	(U)SIM-RPM01 (See annex A)
Test Procedure	1. Power on IoT Device. 2. Wait for ‘Location Update Request’ from IoT Device/ IoT communication module. 3. Accept the Location Update. 4. When IoT Device attempts GPRS Attach, Reject it with GMM #7 (No PS services allowed). 5. Accept next Location Update Request and GPRS Attach Request. 6. Power OFF IoT Device.
Exit Criteria	1. Verify IoT Device does not send LU/Attach before T1 (+/-15%) after step 4.

	2. Verify IoT Device attempts LU/Attach after T1 (+/-15%) expires. 3. Verify IoT Device increments counter C-R-1 by 1.

5.4.9.3 TC-RMM6c

Purpose	RPM waits for time T1 and resets the modem after permanent EMM reject.
Requirement under test	RMM6, RMM7, RTC1
Entry Criteria	1. IoT Device application supports RPM features.
(U)SIM Parameter Settings	(U)SIM-RPM01 (See annex A)
Test Procedure	1. Power ON IoT Device. 2. Reject Attach Request with EMM cause #7 (EPS services not allowed).
Exit Criteria	1. Verify IoT Device does not send Attach before T1 (+/-15%) after step 2. 2. Verify IoT Device attempts Attach after T1 (+/-15%) expires. 3. Verify IoT Device increments counter C-R-1 by 1.

5.4.10 TC-RMM9

Purpose	Service requests will not trigger additional registration attempts.
Requirement under test	RMM9
Entry Criteria	1. IoT communication module supports RPM feature.
(U)SIM Parameter Settings	(U)SIM-RPM01 (See annex A)
Test Procedure	1. Enable a cell (T3212 Periodic Registration Timer = 30 mins) on Network. 2. Power on IoT Device. 3. Confirm that the IoT Device attempts LOCATION UPDATE procedure which is ignored and then waits T3210 (20s). 4. Step 3 is repeated 3 more times with a gap of T3211 (15s) in between. 5. Issues 3 AT commands in 3 minutes (evenly spaced) to initiate packet session. 6. Power off IoT Device and deactivate the cell.
Exit Criteria	1. Confirm that IoT Device does NOT attempt any LOCATION UPDATE procedure after step 5.

5.4.11 TC-RMM10

Purpose	Service requests will not trigger additional registration attempts.
Requirement under test	RMM10
Entry Criteria	1. IoT Device application supports RPM features
(U)SIM Parameter Settings	(U)SIM-RPM04 (See annex A)

Test Procedure	1. Enable a cell (T3302 = 12 mins) on Network. 2. Power ON IoT Device. 3. IoT Device performs Location Update successfully. 4. Confirm that the IoT Device attempts 5 GPRS ATTACH procedures T3310 (15s) apart each of which is ignored. The IoT Device shall then wait T3311 (15s). 5. Step 4 will be repeated 4 more times. 6. Issues 3 AT commands in 3 minutes (evenly spaced) to initiate packet session. 7. Power OFF IoT Device.
Exit Criteria	1. Confirm that IoT Device does NOT attempt any LOCATION UPDATE or GPRS Attach procedure in step 6.

5.4.12 TC-RSM1

Purpose	RPM controls # of PDP context activation requests in PDP ignore scenario.
Requirement under test	RSM1, RSM2, RSM7
Entry Criteria	1. IoT communication module supports RPM feature.
(U)SIM Parameter Settings	(U)SIM-RPM02 (See annex A)
Test Procedure	1. Power on, successful registration. 2. SS sends AT command to initiate packet session on a specific APN. 3. PDP Context Activation Requests from IoT Device are ignored by SS. 4. SS issues (2xF1)/5 AT commands to initiate packet session on the same APN in a period of 1 hour (evenly distributed) and ensure all PDP requests received from IoT Device are ignored by the network.
Exit Criteria	1. Verify that the number of PDP Activation Requests sent to the network every 15 minutes is greater than or equal to MAX (0.05*F1, 1). 2. Verify IoT Device has sent a total of no more than F1 PDP Activation Requests in an hour. 3. Verify C-PDP counter is incremented each time the PDP Context Activation Request is ignored.

5.4.13 TC-RSM3

Purpose	RPM controls # of PDP context activation requests in "permanent" PDP reject scenario.
Requirement under test	RSM3, RSM4, RSM7
Entry Criteria	1. IoT communication module supports RPM feature.
(U)SIM Parameter Settings	(U)SIM-RPM01 (See annex A)
Test Procedure	1. Power on IoT Device, successful registration. 2. SS sends AT command to initiate packet session on a specific APN.

	3. PDP Context Activation Requests from IoT Device are rejected by SS with cause SM# 33 (Requested Service Option Not Subscribed). 4. SS issues 2xF2 AT commands to initiate packet session on the same APN per hour for a period of 2 hour (evenly distributed) and ensure all PDP requests received from IoT Device are rejected with SM#33.
Exit Criteria	1. Verify that the number of PDP Activation Requests sent to the network every 15 minutes is greater than or equal to MAX (0.05*F2, 1). 2. Verify IoT Device sends less than F2 PDP Activation Requests in an hour. 3. Verify IoT Device sends less PDP Activation Requests in the second hour than the first hour. 4. Verify C-PDP-2 counter is incremented each time the PDP Context Activation Request is ignored.

5.4.14 TC-RSM5

Purpose	RPM controls # of PDP context activation requests in "temporary" PDP reject scenario. UE uses default parameters when RPM parameters NOT present on the (U)SIM.
Requirement under test	RSM5, RSM6, RSM7
Entry Criteria	1. IoT communication module supports RPM feature. 2. There are no RPM parameters on the (U)SIM.
(U)SIM Parameter Settings	(U)SIM-RPM04 (See annex A)
Test Procedure	1. Power on IoT Device, successful registration. 2. SS sends AT command to initiate packet session on a specific APN. 3. UE sends PDP Context Activation Request, which is rejected by SS with cause SM# 26 (Insufficient Resources). 4. SS Issue 2xF3 PDP Activation Requests to the same APN in an hour (evenly distributed) and ensure all PDP requests received from IoT Device are rejected with SM #26 by the network.
Exit Criteria	1. Verify that the number of PDP Activation Requests sent to the network every 15 minutes is greater than or equal to MAX (0.05*F3, 1) 2. Verify IoT Device has sent less than F3 PDP Activation Requests in an hour 3. Verify C-PDP-3 counter is incremented each time the PDP Context Activation Request is ignored.

5.4.15 TC-RSM8

Purpose	Checks IoT Device behaviour when application attempts to frequently activate & deactivate PDP context to the same APN. UE uses default parameters when RPM parameters NOT present on the USIM.
Requirement under test	RSM8

Entry Criteria	1. IoT communication module supports RPM feature. 2. There is no RPM parameters on the USIM.
(U)SIM Parameter Settings	(U)SIM-RPM04 (See annex A)
Test Procedure	1. Power on IoT Device, successful registration. 2. SS sends AT command to activate PDP context on a specific APN; then deactivate the PDP context. This is done 2*F4 times in an hour. 3. Verify IoT Device sends a max of F4 PDP Activation to the same APN within the hour.
Exit Criteria	1. Verify IoT Device sends a max of F4 PDP Activation to the same APN within the hour. 2. Verify C-PDP-4 counter is incremented each time the PDP Context Activation Request is ignored.

5.4.16 TC-RTC4

Purpose	Verify the periodic Decrement of RPM operation management counters.
Requirement under test	RTC4, RTC5, RTC6
Entry Criteria	1. IoT Device is powered off. 2. RPM parameters are present on (U)SIM card and set as follows: a. RPM_Enabled_Flag = ON b. LR1 leak rate for C-BR-1 = 0 c. LR2 leak rate for C-R-1 = 2 d. LR3 leak rate for C-PDP-1 TO C-PDP-4 = 1 e. C-BR-1 Counter related to N1 f. C-BR-1 Counter related to N1 - 0A g. C-R-1 Counter related to T1 - 14 h. C-PDP-1 Counter related to F1 - 00 i. C-PDP-2 Counter related to F2 - 01 j. C-PDP-3 Counter related to F3 - 64 k. C-PDP-4 Counter related to F4 - FF
(U)SIM Parameter Settings	(U)SIM-RPM06 (See annex A)
Test Procedure	1. Power on the IoT Device for 2.5 hours. 2. Verify counters in file "EF-RPM Operational management Counters". 3. Power off the IoT Device.
Exit Criteria	1. Verify that a. C-BR-1 is NOT decremented. b. C-R-1 is decremented by 1. c. C-PDP-1 and C-PDP-2 are 0; C-PDP-3 and C-PDP-4 are decremented by 2.

5.4.17 TC-RTC7

Purpose	Verify "EF-RPM Operational Management Counters" can be read through OTA
Requirement under test	RTC7

Entry Criteria	1. IoT Device application supports RPM features.
	2. RPM parameters are present on SIM card (RPM_Enabled_Flag = ON).
	3. Set following RPM Operational Management Counters to:
	a. C-BR-1 = 10; C-R-1 = 20;
	b. C-PDP-1 = 0; C-PDP-2 = 1;
	c. C-PDP-3 = 100; C-PDP-4 = 255;

(U)SIM Parameter Settings	(U)SIM-RPM06 (See annex A)
Test Procedure	1. Activate the cell. 2. Power ON IoT Device. 3. Accept Location Update Request and GPRS Attach Request. 4. Wait for 5 minutes. 5. Send OTA message to read "EF-RPM Operational Management Counters". 6. Power OFF U IoT Device.

Exit Criteria	1. Verify that:
	a. C-BR-1 = 10; C-R-1 = 20;
	b. C-PDP-1 = 0; C-PDP-2 = 1;
	c. C-PDP-3 = 100; C-PDP-4 = 255;

5.4.18 TC-RTC8

Purpose	Verify RPM (U)SIM Parameters
Requirement under test	RTC8
Entry Criteria	1. (U)SIM supports RPM feature
(U)SIM Parameter Settings	(U)SIM-RPM0 (See annex A)
Test Procedure	1. Read RPM parameters from (U)SIM with Card Reader.
Exit Criteria	1. Verify that following files are present on (U)SIM: a. DF-ARMED AGENT - 3F00/7F66/5F40 b. EF-RPM Enabled Flag - 3F00/7F66/5F40/4F40 c. EF-RPM Parameters - 3F00/7F66/5F40/4F41 d. EF-RPM Operational Management Counters Leak Rate – e. 3F00/ 7F66/5F40/ f. EF-RPM Operational Management Counters - 3F00/7F66/5F40/4F43 g. EF-RPM Version Information 3F00/7F66/5F40/4F44

Annex A (U)SIM Settings for Radio Policy Manager Test Cases

(U)SIM Settings ID	**(U)SIM-RPM01**	**(U)SIM-RPM02**	**(U)SIM-RPM03**	**(U)SIM-RPM04**	**(U)SIM-RPM06**	**(U)SIM-RPM11**
IMSI	HPLMN	HPLMN	HPLMN	HPLMN	HPLMN	HPLMN
RPM Parameters Status	Present on USIM	Present on USIM	Present on USIM	**NOT** present on USIM	Present on USIM	Present on USIM
RPM Parameter Name	**Test Value**	**Test Value**	**Test Value**	**Test Value**	**Test Value**	**Test Value**
RPM_Flag	1 (ON)	1 (ON)	0 (OFF)	N/A	1 (ON)	1 (ON)
N1	6	6	6	N/A	6	0
T1	6 Minutes	30 Minutes	6 Minutes	N/A	6 Minutes	0
F1	60	60	60	N/A	60	60
F2	30	30	30	N/A	30	30
F3	60	60	60	N/A	60	60
F4	30	30	30	N/A	30	30
LR-1	0	0	0	N/A	0	0
LR-2	0	0	0	N/A	2	0
LR-3	0	0	0	N/A	1	0
C-BR-1	x	x	x	N/A	10	x
C-R-1	x	x	x	N/A	20	x
C-PDP-1	x	x	x	N/A	0	x
C-PDP-2	x	x	x	N/A	1	x
C-PDP-3	x	x	x	N/A	100	x
C-PDP-4	x	x	x	N/A	255	x
RPM Version Implemented	0	0	0	N/A	0	0

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	12 December 2014	New PRD IoT Device Connection Efficiency Common Test Cases	CLP/PSMC	Ian Smith/GSMA

B.2 Other Information

Type	Description
Document Owner	CLP/PSMC
Editor / Company	Ian Smith/GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.