

IoT Device Connection Efficiency Test Book
Version 7.0
02 October 2023

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document 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

Copyright © 2023 GSM Association

Disclaimer

The GSMA 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.

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction 3
1.1 Problem Statement 3
1.2 Document Scope 3
1.3 Intended Use of the Document 3
1.3.1 Mobile Network Operators 3
1.3.2 IoT Service Providers 3
1.3.3 IoT Device Maker 3
1.3.4 IoT Device Application Developer 4
1.3.5 Communication Module Vendor 4
1.3.6 Radio Baseband Chipset Vendor 4
1.4 Definition of Terms 4
1.5 Abbreviations 6
1.6 References 7
2 IoT Device Approval Framework 8
3 Test Environment 8
3.1 Controlled Mobile Network 8
3.2 Simulated Mobile Network 9
3.3 Live Mobile Network 9
4 Mapping of Test Cases to Requirements 10
5 Test Cases 18
5.1 IoT Device Application Test Cases 18
5.2 Communications Module Test Cases 32
5.2.1 IPv6 Test Cases 32
5.2.2 Fast Dormancy Test Case 34
5.2.3 Security Test Cases 35
5.2.4 Subscription Identifier Test Cases 36
5.2.5 IoT Device Host Identity Reporting (DHIR) Test Cases 37
5.3 Void 45
5.4 Radio Policy Manager Test Cases 45
Annex A (U)SIM Settings for Radio Policy Manager Test Cases 59
Annex B Test Applicability and Classification 61
Annex C Test Applicability and Classification for certification Organisations. 2
Annex D Document Management 4
D.1 Document History 4
D.2 Other Information 5

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

Term	Description
Back-off Timer	The Back-off Timer is a dynamic timer which value is based on a unique value for the device (desirably the IMSI) and the number of consecutive failures (which points to different Back-off Base Intervals).
Communications Module	The communications component which provides wide area (2G, 3G, 4G) radio connectivity. Comprising of Communications Module Firmware, Radio Baseband Chipset and UICC
Communications Module Firmware	The functionality within the Communications Module that provides an API to the IoT Device Application and controls the Radio Baseband Chipset.
Fast Dormancy	Device power saving mechanism. See GSMA TS.18 [14].
Global Certification Forum	An independent worldwide certification scheme for mobile phones and wireless devices that are based on 3GPP standards. The GCF provides the framework within which cellular GSM, UMTS and LTE mobile devices and Communication Modules obtain certification for use on GCF Mobile Network Operators' networks. Obtaining GCF Certification on a mobile device ensures compliance with 3GPP network standards within the GCF Mobile Network Operators' networks. Consequently, GCF Mobile Network Operators may block devices from their network if they are not GCF certified. For more information, see http://www.globalcertificationforum.org
Internet of Things	The Internet of Things describes the coordination of multiple machines, devices and appliances connected to the Internet through multiple networks. These devices include everyday objects such as tablets and consumer electronics, and other machines such as vehicles, monitors and sensors equipped with machine-to-machine (M2M) communications that allow them to send and receive data.

Term	Description
IoT Device	The combination of both the IoT Device Application and the Communications Module.
IoT Device Application	The application software component of the IoT Device that controls the Communications Module and interacts with an IoT Service Platform via the Communications Module.
IoT Device Host	The application specific environment containing the IoT Device e.g. vehicle, utility meter, security alarm etc.
IoT Server Application	An application software component that runs on a server and can exchange data and interact with the IoT Devices and the IoT Device Applications over the IoT Service Platform.
IoT Service	The IoT service provided by the IoT Service Provider.
IoT Service Platform	The service platform, hosted by the IoT Service Provider which communicates to an IoT Device to provide an IoT Service. The IoT Service Platform can exchange data with the IoT Device Application over the Mobile Network and through the Communication Module, using (among others) IP-based protocols over a packet-switched data channel. Also, the IoT Service Platform typically offers Device Management capabilities, acting as a so-called Device Management Server. Finally, the IoT Service Platform typically offers APIs for IoT Server Applications to exchange data and interact with the IoT Device Applications over the IoT Service Platform.
IoT Service Provider	The provider of IoT services working in partnership with a Mobile Network Operator to provide an IoT Service to an End Customer. The provider could also be a Mobile Network Operator.
Machine to Machine	Machine-to-Machine (M2M) is an integral part of the Internet of Things (IoT) and describes the use of applications that are enabled by the communication between two or more machines. M2M technology connects machines, devices and appliances together wirelessly via a variety of communications channels, including IP and SMS, to deliver services with limited direct human intervention turning these devices into intelligent assets that open up a range of possibilities for improving how businesses are run.
Mobile Network Operator	The mobile network operator(s) connecting the IoT Device Application to the IoT Service Platform.

Term	Description
PTCRB	The independent body established as the wireless device certification forum by North American Mobile Network Operators. The PTCRB provides the framework within which cellular GSM, UMTS and LTE mobile devices and Communication Modules obtain certification for use on PTCRB Mobile Network Operator networks. Obtaining PTCRB Certification on a mobile device ensures compliance with 3GPP network standards within the PTCRB Mobile Network Operators' networks. Consequently, PTCRB Mobile Network Operators may block devices from their network if they are not PTCRB certified. For more information, see http://ptcrb.com
Radio Baseband Chipset	The functionality within the Communications Module that provides connectivity to the mobile network.
Test case:- TS35_X.X_TC_YYY	TS.35 = this PRD number. X.X = the section number the test case can be found in. TC = Test Case YYY = the test case number.
UICC	The smart card used by a mobile network to authenticate devices for connection to the mobile network and access to network services.

1.5 Abbreviations

Abbreviation	Description
3GPP	3rd Generation Project Partnership
API	Application Programming Interface
APN	Access Point Name
GCF	Global Certification Forum
GSM	Global System Mobile
GSMA	GSM Association
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
LTE	Long Term Evolution
M2M	Machine to Machine

Abbreviation	Description
NAT	Network Address Translation
NFM	Network Friendly Mode
OTA	Over The Air
PDP	Packet Data Protocol
PTCRB	A pseudo-acronym, originally meaning PCS Type Certification Review Board, but no longer applicable.
RPM	Radio Policy Manager
RRC	Radio Resource Control
SMS	Short Message Service
SS	System Simulator
UMTS	Universal Mobile Telecommunications Service
(U)SIM	(Universal) Subscriber Identity Module
USB	Universal Serial Bus

1.6 References

Ref	Document Title	Document Location
1	CLNE.03 GSMA IoT Device Connection Efficiency Guidelines	www.gsma.com
2	GSMA TS.24 “Operator Minimum Acceptance Values for Device Antenna Performance”	www.gsma.com
3	3GPP TS 31.102 Characteristics of the Universal Subscriber Identity Module (USIM) application	www.3gpp.org

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 (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)

3.1 Controlled Mobile Network

This kind of test environment is typically used for operator lab acceptance.

Test verdicts are set manually.

The test setup is dedicated to one specific operator or network equipment vendor.

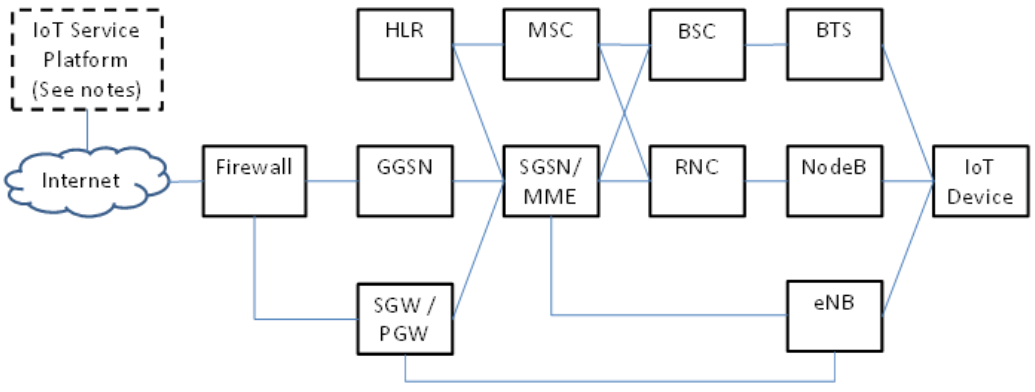

Figure 1: A typical configuration of a 'controlled' mobile network environment in a lab

Note: For the testing of IoT Device Application requirements, an actual or simulated IoT Service Platform is necessary. A simulated IoT Service Platform does not need to actually

implement the service logic of an actual IoT Service Platform, but needs at least to return predefined valid responses to requests sent to it by the IoT Device Application over the controlled mobile network.

Note: For the testing of Communication Module requirements, no IoT Service Platform is needed.

3.2 Simulated Mobile Network

This kind of test environment is typically used for conformance testing.

Test verdicts are set automatically.

The test setup is applicable for all operators.

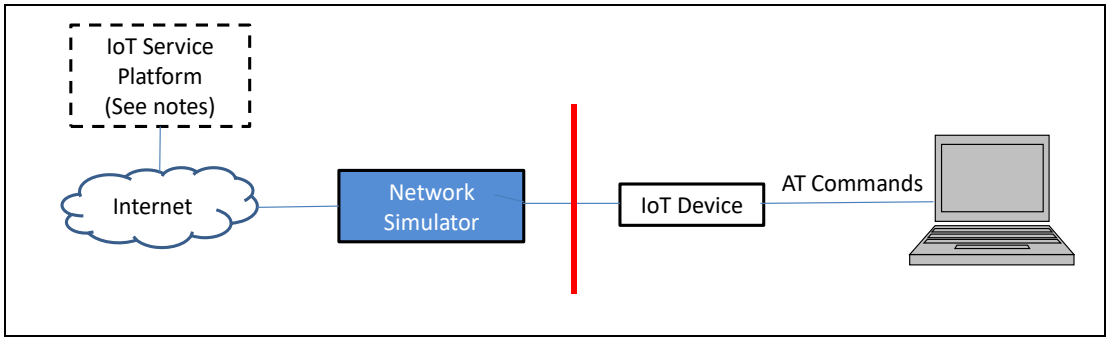

Figure 2: A typical configuration of a conformance test in a "simulated mobile network environment"

Note: For the testing of IoT Device Application requirements, an actual or simulated IoT Service Platform is necessary. A simulated IoT Service Platform does not need to actually implement the service logic of an actual IoT Service Platform, but needs at least to return predefined valid responses to requests sent to it by the IoT Device Application over the simulated mobile network.

Note: For the testing of Communication Module requirements, a reference IoT Device Application with a known behaviour will be typically used.

3.3 Live Mobile Network

This kind of test environment is typically used in two cases:

1. By a Communication Module vendor, before sending the module for lab testing, in order to minimize the risk of test failures as well as lab testing costs and lab testing time. The IoT Device used could be configured with specific parameters 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.
2. By a solution integrator, to perform tests on a solution that uses pre-certified components, before its mass deployment, in order to check the expected operation of this overall solution in conditions as close as possible to the live production environment (including particular locations or machines).

Test verdict are set manually.

The test setup is applicable for the target operator only.

For the testing of IoT Device Application requirements, an actual IoT Service Platform is necessary.

For the testing of Communication Module requirements, the target IoT Device Application is typically used.

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 **Error! Reference source not found.** of this d ocument.

IoT Device Connection Efficiency Guidelines Section		Requirement	Test Case	Comments
3	IoT Device Requirements	TS.34_3.0_REQ_001	-	High level requirement.
		TS.34_3.0_REQ_002	-	High level requirement.
		TS.34_3.0_REQ_003	-	See GSMA TS.24 [2].
		TS.34_3.0_REQ_004	-	High level requirement.
4	IoT Device Application Requirements	TS.34_4.0_REQ_001	TS35_5.1_TC_001	
		TS.34_4.0_REQ_002	TS35_5.1_TC_002	
		TS.34_4.0_REQ_003	TS35_5.1_TC_003	
		TS.34_4.0_REQ_004	-	For future study
		TS.34_4.0_REQ_005	TS35_5.1_TC_004a TS35_5.1_TC_004b	
		TS.34_4.0_REQ_006 TS.34_4.0_REQ_006.1 TS.34_4.0_REQ_006.2	TS35_5.1_TC_005	
		TS.34_4.0_REQ_007	TS35_5.1_TC_006	
		TS.34_4.0_REQ_008	TS35_5.1_TC_007	
		TS.34_4.0_REQ_009	TS35_5.1_TC_007	
		TS.34_4.0_REQ_010	-	For future study
		TS.34_4.0_REQ_011 TS.34_4.0_REQ_011.1 TS.34_4.0_REQ_011.2	TS35_5.1_TC_008a TS35_5.1_TC_008b TS35_5.1_TC_008c TS35_5.1_TC_008d TS35_5.1_TC_008e TS35_5.1_TC_008f TS35_5.1_TC_008g TS35_5.1_TC_008h TS35_5.1_TC_008i	

IoT Device Connection Efficiency Guidelines Section		Requirement	Test Case	Comments
		TS.34_4.0_REQ_012 TS.34_4.0_REQ_012.1 TS.34_4.0_REQ_012.2 TS.34_4.0_REQ_012.3	TS35_5.1_TC_009	
		TS.34_4.0_REQ_013 TS.34_4.0_REQ_013.1 TS.34_4.0_REQ_013.2 TS.34_4.0_REQ_013.3	TS35_5.1_TC_010	
		TS.34_4.0_REQ_014 TS.34_4.0_REQ_014.1	TS35_5.1_TC_011	
		TS.34_4.0_REQ_015	-	For future study
		TS.34_4.0_REQ_016	TS35_5.1_TC_012	
		TS.34_4.0_REQ_017	-	For future study
		TS.34_4.0_REQ_018	-	For future study
		TS.34_4.0_REQ_019	TS35_5.1_TC_013	
		TS.34_4.0_REQ_020	TS35_5.1_TC_014	
		TS.34_4.0_REQ_021	TS35_5.1_TC_015a TS35_5.1_TC_015b	
		TS.34_4.0_REQ_022 TS.34_4.0_REQ_022.1	TS35_5.1_TC_016a TS35_5.1_TC_016b	
		TS.34_4.0_REQ_023	-	
		TS.34_4.0_REQ_024	TS35_5.1_TC_017	
		TS.34_4.0_REQ_025	TS35_5.1_TC_018	
		TS.34_4.0_REQ_026	-	For future study
		TS.34_4.0_REQ_027	-	For future study
		TS.34_4.0_REQ_028	-	For future study
		TS.34_4.0_REQ_029 TS.34_4.0_REQ_029.1		For future study
5.1	Standards Compliance	TS.34_5.1_REQ_001	-	Out of scope
		TS.34_5.1_REQ_002	-	Out of scope
		TS.34_5.1_REQ_003	-	Out of scope
5.2	Network Efficiency Requirements	TS.34_5.2_REQ_001	-	High level requirement
		TS.34_5.2_REQ_002	-	For future study
		TS.34_5.2_REQ_003	-	Out of scope
5.3	Requirements for Communication Modules that Support IPv6	TS.34_5.3_REQ_001	TS35_5.2.1_TC_001	

IoT Device Connection Efficiency Guidelines Section		Requirement	Test Case	Comments
		TS.34_5.3_REQ_002	TS35_5.2.1_TC_002	
		TS.34_5.3_REQ_003	TS35_5.2.1_TC_003	
		TS.34_5.3_REQ_004	TS35_5.2.1_TC_004	
		TS.34_5.3_REQ_005	TS35_5.2.1_TC_005	
5.4	Requirements for Communication Modules that Support LTE	TS.34_5.4_REQ_001	-	Out of scope
5.5	Requirements for Communication Modules that Support Fast Dormancy	TS.34_5.5_REQ_001 TS.34_5.5_REQ_002	TS35_5.2.2_TC_001	
5.6	(U)SIM Interface Requirements	TS.34_5.6_REQ_001	-	Out of scope
		TS.34_5.6_REQ_002	-	Out of scope
5.7	Security Requirements	TS.34_5.7_REQ_001	-	High level requirement
		TS.34_5.7_REQ_002 TS.34_5.7_REQ_002.1	TS35_5.2.3_TC_001	
		TS.34_5.7_REQ_003	-	For future study
		TS.34_5.7_REQ_004 TS.34_5.7_REQ_005	TS35_5.2.3_TC_002	
5.8	Device Management	TS.34_5.8_REQ_001	-	High level requirement
		TS.34_5.8_REQ_002	-	High level requirement
		TS.34_5.8_REQ_003	TS35_5.1_TC_017	
		TS.34_5.8_REQ_004	TS35_5.1_TC_018	
5.9	Subscription Identifier Requirements	TS.34_5.9_REQ_001	TS35_5.2.4_TC_001	
		TS.34_5.9_REQ_002	TS35_5.2.4_TC_002	
5.10	Device Host Identity Reporting	TS.34_5.10_REQ_001	TS35_5.2.5_TC_001 TS35_5.2.5_TC_002 TS35_5.2.5_TC_003	
		TS.34_5.10_REQ_002 TS.34_5.10_REQ_002.1	TS35_5.2.5_TC_001	
		TS.34_5.10_REQ_003 TS.34_5.10_REQ_003.1 TS.34_5.10_REQ_003.2	TS35_5.2.5_TC_001	

IoT Device Connection Efficiency Guidelines Section		Requirement	Test Case	Comments
		TS.34_5.10_REQ_004 TS.34_5.10_REQ_004.1	TS35_5.2.5_TC_007	
		TS.34_5.10_REQ_005 TS.34_5.10_REQ_005.1	TS35_5.2.5_TC_007	
		TS.34_5.10_REQ_006 TS.34_5.10_REQ_006.1 TS.34_5.10_REQ_006.2 TS.34_5.10_REQ_006.3	TS35_5.2.5_TC_007	
		TS.34_5.10_REQ_007 TS.34_5.10_REQ_007.1	TS35_5.2.5_TC_007	
		TS.34_5.10_REQ_008		For future study
		TS.34_5.10_REQ_009		For future study
		TS.34_5.10_REQ_010		For future study
		TS.34_5.10_REQ_011		For future study
		TS.34_5.10_REQ_01.1		For future study
		TS.34_5.10_REQ_012		For future study
		TS.34_5.10_REQ_013		For future study
		TS.34_5.10_REQ_013.1		For future study
		TS.34_5.10_REQ_014 TS.34_5.10_REQ_014.1	TS35_5.2.5_TC_013	
		TS.34_5.10_REQ_015		For future study
		TS.34_5.10_REQ_016		For future study
		TS.34_5.10_REQ_017		For future study
		TS.34_5.10_REQ_018		For future study
		TS.34_5.10_REQ_019		For future study
		TS.34_5.10_REQ_020		For future study
		TS.34_5.10_REQ_021		For future study
		TS.34_5.10_REQ_022	TS35_5.2.5_TC_006	
		TS.34_5.10_REQ_023	TS35_5.2.5_TC_006	
		TS.34_5.10_REQ_024	TS35_5.2.5_TC_009	
		TS.34_5.10_REQ_025 TS.34_5.10_REQ_025.1	TS35_5.2.5_TC_005	
		TS.34_5.10_REQ_026 TS.34_5.10_REQ_026.1 TS.34_5.10_REQ_026.2 TS.34_5.10_REQ_026.3 TS.34_5.10_REQ_026.4	TS35_5.2.5_TC_011	

IoT Device Connection Efficiency Guidelines Section		Requirement	Test Case	Comments
		TS.34_5.10_REQ_027 TS.34_5.10_REQ_027.1 TS.34_5.10_REQ_027.2 TS.34_5.10_REQ_027.3 TS.34_5.10_REQ_027.4 TS.34_5.10_REQ_027.5 TS.34_5.10_REQ_027.6	TS35_5.2.5_TC_012	
		TS.34_5.10_REQ_028	TS35_5.2.5_TC_010	
		TS.34_5.10_REQ_029 TS.34_5.10_REQ_029.1	TS35_5.2.5_TC_008	
		TS.34_5.10_REQ_030	TS35_5.2.5_TC_010	
		TS.34_5.10_REQ_031	TS35_5.2.5_TC_010	
		TS.34_5.10_REQ_032	TS35_5.2.5_TC_010	
		TS.34_5.10_REQ_033	TS35_5.2.5_TC_004	
5.11	Communication Modules that Support 5G	TS.34_5.11_REQ_001	-	For future study
6	IoT Service Provider Requirements	TS.34_6.0_REQ_001	-	For future study
		TS.34_6.0_REQ_002 TS.34_6.0_REQ_002.1 TS.34_6.0_REQ_002.2	-	Out of scope
		TS.34_6.0_REQ_003	-	For future study
		TS.34_6.0_REQ_004	-	For future study
		TS.34_6.0_REQ_005 TS.34_6.0_REQ_005.1	-	For future study
7	Policy Based Connection Efficiency Requirements			
7.2.1	General Mechanism	TS.34_7.2.1 _REQ_001	-	For future study
		TS.34_7.2.1_REQ_002	-	For future study
		TS.34_7.2.1_REQ_003	-	For future study
7.2.2	Policy Management	TS.34_7.2.2 _REQ_001	-	For future study
		TS.34_7.2.2_REQ_002	-	For future study
8.2.1	Radio Policy Manager - General	TS.34_8.2.1_REQ_001	TS35_5.4_TC_001	
		TS.34_8.2.1_REQ_002 TS.34_8.2.1_REQ_002.1	TS35_5.4_TC_002	
		TS.34_8.2.1_REQ_003	TS35_5.4_TC_003	

IoT Device Connection Efficiency Guidelines Section		Requirement	Test Case	Comments
		TS.34_8.2.1_REQ_004	TS35_5.4_TC_004	
		TS.34_8.2.1_REQ_005	TS35_5.4_TC_005a TS35_5.4_TC_005b TS35_5.4_TC_005c	
		TS.34_8.2.1_REQ_006 TS.34_8.2.1_REQ_006.1 TS.34_8.2.1_REQ_006.2 TS.34_8.2.1_REQ_006.3	TS35_5.4_TC_006	
		TS.34_8.2.1_REQ_007	TS35_5.4_TC_001 TS35_5.4_TC_002 TS35_5.4_TC_003	
		TS.34_8.2.1_REQ_008	TS35_5.4_TC_002	
		TS.34_8.2.1_REQ_009	TS35_5.4_TC_001 TS35_5.4_TC_003	
8.2.2	Radio Policy Manager - Mobility Management	TS.34_8.2.2_REQ_001	-	High level requirement.
		TS.34_8.2.2_REQ_002	TS35_5.4_TC_007	
		TS.34_8.2.2_REQ_003 TS.34_8.2.2_REQ_003.1	TS35_5.4_TC_008a TS35_5.4_TC_008b TS35_5.4_TC_008c	
		TS.34_8.2.2_REQ_004 TS.34_8.2.2_REQ_004.1	TS35_5.4_TC_008a TS35_5.4_TC_008b	
		TS.34_8.2.2_REQ_005 TS.34_8.2.2_REQ_005.1	TS35_5.4_TC_008a	
		TS.34_8.2.2_REQ_006 TS.34_8.2.2_REQ_006.1 TS.34_8.2.2_REQ_006.2	TS35_5.4_TC_009a TS35_5.4_TC_009b TS35_5.4_TC_009c	
		TS.34_8.2.2_REQ_007 TS.34_8.2.2_REQ_007.1	TS35_5.4_TC_009a TS35_5.4_TC_009b TS35_5.4_TC_009c	
		TS.34_8.2.2_REQ_008	TS35_5.4_TC_005b	
		TS.34_8.2.2_REQ_009	TS35_5.4_TC_010	
		TS.34_8.2.2_REQ_010	TS35_5.4_TC_011	
		TS.34_8.2.2_REQ_011	TS35_5.4_TC_019	
8.2.3	Radio Policy Manager – Session Management	TS.34_8.2.3_REQ_001	TS35_5.4_TC_012	
		TS.34_8.2.3_REQ_002 TS.34_8.2.3_REQ_002.1	TS35_5.4_TC_012	

IoT Device Connection Efficiency Guidelines Section		Requirement	Test Case	Comments
		TS.34_8.2.3_REQ_003 TS.34_8.2.3_REQ_003.1	TS35_5.4_TC_013	
		TS.34_8.2.3_REQ_004 TS.34_8.2.3_REQ_004.1	TS35_5.4_TC_013	
		TS.34_8.2.3_REQ_005 TS.34_8.2.3_REQ_005.1	TS35_5.4_TC_014	
		TS.34_8.2.3_REQ_006 TS.34_8.2.3_REQ_006.1	TS35_5.4_TC_014	
		TS.34_8.2.3_REQ_007	TS35_5.4_TC_012 TS35_5.4_TC_013 TS35_5.4_TC_014	
		TS.34_8.2.3_REQ_008 TS.34_8.2.3_REQ_008.1 TS.34_8.2.3_REQ_008.2	TS35_5.4_TC_015	
		TS.34_8.2.3_REQ_009 TS.34_8.2.3_REQ_009.1	TS35_5.4_TC_015	
8.2.4	Timers and Counters	TS.34_8.2.4_REQ_001	TS35_5.4_TC_009a TS35_5.4_TC_009b TS35_5.4_TC_009c	
		TS.34_8.2.4_REQ_002	-	For future study
		TS.34_8.2.4_REQ_003 TS.34_8.2.4_REQ_003.1	-	For future study
		TS.34_8.2.4_REQ_004 TS.34_8.2.4_REQ_004.1 TS.34_8.2.4_REQ_004.2	TS35_5.4_TC_016	
		TS.34_8.2.4_REQ_005 TS.34_8.2.4_REQ_005.1 TS.34_8.2.4_REQ_005.2	TS35_5.4_TC_016	
		TS.34_8.2.4_REQ_006 TS.34_8.2.4_REQ_006.1 TS.34_8.2.4_REQ_006.2	TS35_5.4_TC_016	
		TS.34_8.2.4_REQ_007	TS35_5.4_TC_017	
		TS.34_8.2.4_REQ_008	TS35_5.4_TC_018	
		TS.34_8.2.4_REQ_009 TS.34_8.2.4_REQ_009.1 TS.34_8.2.4_REQ_009.2	TS35_5.4_TC_005a TS35_5.4_TC_005b TS35_5.4_TC_005c	
		TS.34_8.2.4_REQ_010	TS35_5.4_TC_001	
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.		

IoT Device Connection Efficiency Guidelines Section		Requirement	Test Case	Comments
9.2	Handling of Low Access Priority Indicator	Please refer to the associated GCF or PTCRB test cases.		
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

A tolerance of +/-15% is permitted for all timers in this section unless stated otherwise.

5.1 IoT Device Application Test Cases

TS35_5.1_TC_001

Purpose	To test the “Always-on” connectivity mechanism for an IoT Device Application that very frequently sends data.
Requirement under test	TS.34_4.0_REQ_001
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.

TS35_5.1_TC_002

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	TS.34_4.0_REQ_002
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.

TS35_5.1_TC_003

Purpose	Check that the IoT Device avoids IoT Device Application timing synchronization.
Requirement under test	TS.34_4.0_REQ_003

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.

TS35_5.1_TC_004a

Purpose	Check the device implements appropriate security measures to prevent unauthorized or insecure local device management.
Requirement under test	TS.34_4.0_REQ_005
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.

TS35_5.1_TC_004b

Purpose	Check the device implements appropriate security measures to prevent unauthorized or insecure remote device management.
Requirement under test	TS.34_4.0_REQ_005

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.

TS35_5.1_TC_005

Purpose	Check the IoT Device Application uses dynamic polling intervals.
Requirement under test	TS.34_4.0_REQ_006, TS.34_4.0_REQ_006.1, TS.34_4.0_REQ_006.2
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.

TS35_5.1_TC_006

Purpose	Check if the IoT Device Application uses a fixed polling interval.
Requirement under test	TS.34_4.0_REQ_007
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.

TS35_5.1_TC_007

Purpose	Check if the IoT Device Application adapts to changes in network communication latency and data speed.
Requirement under test	TS.34_4.0_REQ_008TS.34_4.0_REQ_009.
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.

TS35_5.1_TC_008

TS35_5.1_TC_008a

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • SIM Subscription placed in a terminated state
Requirement under test	TS.34_4.0_REQ_011, TS.34_4.0_REQ_011.1, TS.34_4.0_REQ_011.2
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’.

TS35_5.1_TC_008b

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • SIM Subscription with roaming not allowed
Requirement under test	TS.34_4.0_REQ_011, TS.34_4.0_REQ_011.1, TS.34_4.0_REQ_011.2
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’.

TS35_5.1_TC_008c

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • SIM Subscription with barred GPRS service

Requirement under test	TS.34_4.0_REQ_011, TS.34_4.0_REQ_011.1, TS.34_4.0_REQ_011.2
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’.

TS35_5.1_TC_008d

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	TS.34_4.0_REQ_011, TS.34_4.0_REQ_011.1, TS.34_4.0_REQ_011.2
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’.

TS35_5.1_TC_008e

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	TS.34_4.0_REQ_011, TS.34_4.0_REQ_011.1, TS.34_4.0_REQ_011.2
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’.

TS35_5.1_TC_008f

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • IoT Service Platform is offline.
Requirement under test	TS.34_4.0_REQ_011, TS.34_4.0_REQ_011.1, TS.34_4.0_REQ_011.2
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’.

TS35_5.1_TC_008g

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • IoT Service Platform's IP address is unreachable.
Requirement under test	TS.34_4.0_REQ_011, TS.34_4.0_REQ_011.1, TS.34_4.0_REQ_011.2
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'.

TS35_5.1_TC_008h

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • SMS Centre unreachable.
Requirement under test	TS.34_4.0_REQ_011, TS.34_4.0_REQ_011.1, TS.34_4.0_REQ_011.2
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'.

TS35_5.1_TC_008i

Purpose	Check IoT Device Application behaviour in situations when network communication requests fail: • Subscription with MO SMS barred.

Requirement under test	TS.34_4.0_REQ_011, TS.34_4.0_REQ_011.1, TS.34_4.0_REQ_011.2
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’.

TS35_5.1_TC_009

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	TS.34_4.0_REQ_012, TS.34_4.0_REQ_012.1, TS.34_4.0_REQ_012.2, TS.34_4.0_REQ_012.3
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.

TS35_5.1_TC_010

Purpose	Check IoT Device Application behaviour when the data volume limit with a certain time period is exceeded.
Requirement under test	TS.34_4.0_REQ_013, TS.34_4.0_REQ_013.1, TS.34_4.0_REQ_013.2, TS.34_4.0_REQ_013.3
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.

TS35_5.1_TC_011

Purpose	Check IoT Device Application reports power failures.
Requirement under test	TS.34_4.0_REQ_014, TS.34_4.0_REQ_014.1,
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.

TS35_5.1_TC_012

Purpose	Check IoT Device Application's use of "off-peak' communication.
Requirement under test	TS.34_4.0_REQ_016DAR16
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.

TS35_5.1_TC_013

Purpose	Check behaviour of IoT Device Application when resetting the Communications Module after any communication failures or error conditions.
Requirement under test	TS.34_4.0_REQ_019
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.

TS35_5.1_TC_014

Purpose	Check behaviour of IoT Device Application in Low power mode
Requirement under test	TS.34_4.0_REQ_020DAR20
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.

TS35_5.1_TC_015

TS35_5.1_TC_015a

Purpose	Check IoT Device Application uses a secure data connection.
Requirement under test	TS.34_4.0_REQ_021
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.

TS35_5.1_TC_015b

Purpose	Check for certificate handshake when establishing a secure data connection
Requirement under test	TS.34_4.0_REQ_021
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.

TS35_5.1_TC_016

Void

TS35_5.1_TC_016a

Purpose	Check IoT Device authentication (based on IMSI) towards IoT Service Platform.
Requirement under test	TS.34_4.0_REQ_022, TS.34_4.0_REQ_022.1
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.

TS35_5.1_TC_016b

Purpose	Check IoT Device authentication (based on specific APN) towards IoT service platform.
Requirement under test	TS.34_4.0_REQ_022, TS.34_4.0_REQ_022.1
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.

TS35_5.1_TC_017

Purpose	Check IoT Device and its Communication Module are “reset to factory settings”.
Requirement under test	TS.34_4.0_REQ_024
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.

TS35_5.1_TC_018

Purpose	Check IoT Device and its Communication Module supports “time resynchronisation” via remote and local connection.
Requirement under test	TS.34_4.0_REQ_025

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

TS35_5.2.1_TC_001

Purpose	Check the IoT Communications Module does not send unsolicited messages
Requirement under test	TS.34_5.3_REQ_001
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.

TS35_5.2.1_TC_002

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

Requirement under test	TS.34_5.3_REQ_002
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.

TS35_5.2.1_TC_003

Purpose	Check the Communications Module management system is IPv6 based
Requirement under test	TS.34_5.3_REQ_003
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.

TS35_5.2.1_TC_004

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	TS.34_5.3_REQ_004
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.

TS35_5.2.1_TC_005

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	TS.34_5.3_REQ_005
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

TS35_5.2.2_TC_001

Purpose	Triggering of the ‘Fast Dormancy algorithm’ within the Communications based on IoT Device data inactivity.
Requirement under test	TS.34_5.5_REQ_001, TS.34_5.5_REQ_002
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

TS35_5.2.3_TC_001

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	TS.34_5.7_REQ_002, TS.34_5.7_REQ_002.1
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.

TS35_5.2.3_TC_002

Purpose	To test that it is possible to lock the Communications Module to a unique (U)SIM.
Requirement under test	TS.34_5.7_REQ_004, TS.34_5.7_REQ_005
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

TS35_5.2.4_TC_001

Purpose	Check whether the Communications Module can support 15 digit Directory Numbers/MSISDNs.
Requirement under test	TS.34_5.9_REQ_001
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.

TS35_5.2.4_TC_002

Purpose	Check whether the Communications Module can support 2 and 3 digit based Mobile Network Codes IMSIs.
Requirement under test	TS.34_5.9_REQ_002

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.

5.2.5 IoT Device Host Identity Reporting (DHIR) Test Cases

TS35_5.2.5_TC_001

Purpose	Verify that the Communication Module's FOTA implementation will pass all applicable FOTA tests in the OMA test specification (OMA ETS).
Requirement under test	TS.34_5.10_REQ_001, TS.34_5.10_REQ_002, TS.34_5.10_REQ_002.1, TS.34_5.10_REQ_003, TS.34_5.10_REQ_003.1, TS.34_5.10_REQ_003.2
Entry Criteria	1. Successful execution of MNO Device Management IOT Program.
Test Procedure	1. Execute IOT Program. 2. Submit IOT reports to MNO for review.
Exit Criteria (Pass Criteria)	1. IOT report has been reviewed / approved by MNO.

TS35_5.2.5_TC_002

Purpose	The purpose of this test is to verify that the module can be successfully bootstrapped (using NETWPIN authentication) in order to communicate to the MNO server.
Requirement under test	TS.34_5.10_REQ_001, TS.34_5.10_REQ_002, TS.34_5.10_REQ_002.1, TS.34_5.10_REQ_003, TS.34_5.10_REQ_003.1, TS.34_5.10_REQ_003.2
Entry Criteria	1. Module (IMEI/IMSI) is configured on the MNO DM. 2. Invoke Factory Reset/Master Reset to ensure the module is clear of any server settings in the 3rd DMAcc node. 3. OTA bootstrap configuration on server is set up for NETWPIN authentication.

Test Procedure	1. Invoke a Factory Reset on the module to wipe out any previously applied OTA bootstrap. 2. Send an OTA bootstrap to the module (Go to Settings, Click on DMBOOT). 3. Check the server for the status of the SMS (which contains the bootstrap) delivered to the module. 4. Send a DM GET to the module. 5. Invoke a Factory Reset on the module to wipe out the installed OTA bootstrap and return the module to the factory bootstrap.
Exit Criteria	1. The DM server shows that the SMS with the OTA bootstrap was delivered to the module. 2. DM GET is successful on MNO DM Server.

TS35_5.2.5_TC_003

Purpose	The purpose of this test is to verify that the module is factory bootstrapped to the MNO DM server and has the correct configuration on the module.
Requirement under test	TS.34_5.10_REQ_001
Entry Criteria	1. Programmable code to expose the values of the factory bootstrap account on the module.
Test Procedure	4. Send a DM GET to the module. 5. Use the programmable code on the module to select and expose the following module configuration values: a. OMA-DM Server URL. b. OMA-DM Server port number.
Exit Criteria (Pass Criteria)	1. DM GET is successful. 2. Production and Lab Server URLs in the factory bootstrap accounts on the module must use the correct MNO URLs. 3. Server port number is set to 443 for https.

TS35_5.2.5_TC_004

Purpose	The purpose of this test is to verify that the module is using secure connection technology that meets contemporary and evolving requirements for authentication and data privacy over the targeted end-to-end connection within the scope of DHIR.
Requirement under test	TS.34_5.10_REQ_033
Entry Criteria	1. Programmable code to expose the values of the factory bootstrap account on the module and test case TC-DHIR3 has been run.

Test Procedure	1. Configure the module with a factory bootstrap account for the OMA-DM server. 2. Locate the certificate on the module and identify the name and type of the certificate. 3. Send a DM GET from the OMA-DM server to the module. 4. Verify from the module side logs that the module used https to connect to the server.
Exit Criteria	1. Module is using a x509 technology based certificate. 2. No “unknown certificate” prompt appears on the module during the processing of the DM GET request. 3. DM GET is successful. 4. Module side logs do not show any certificate exception errors. 5. Module side logs show that the module used https to connect to the server.

TS35_5.2.5_TC_005

Purpose	The purpose of this test is to verify that the module is using the designated APN as per the requirements of the MNO.
Requirement under test	TS.34_5.10_REQ_025, TS.34_5.10_REQ_025.1
Entry Criteria	1. Module is configured to use the designated APN for all sessions with the MNO DM server. 2. Test case DHIR3 has been executed successfully. 3. Only a factory bootstrap account is provisioned on the module.
Test Procedure	1. Configure the module with a factory bootstrap account on the server. 2. Send a DM GET to the module. 3. Verify from the module side logs or AT command that the module used the designated APN when routing to the DM Server.
Exit Criteria (Pass Criteria)	1. DM GET is successful (light is green for the request) 2. Module side logs show the module used the designated APN to route to the MNO DM Server per the MNO requirements.

TS35_5.2.5_TC_006

Purpose	Verify that the module correctly reports its module details to the server.
Requirement under test	TS.34_5.10_REQ_022, TS.34_5.10_REQ_023
Entry Criteria	1. Test case DHIR3has been executed successfully. 2. Only a factory bootstrap account is provisioned on the module.

Test Procedure	1. Configure the module with a factory bootstrap account on the server. 2. Send a DM GET Check ALL to the module. 3. Look up the module details on the server in the following locations: a. Protection & Control > Details > DM Tree > Filter ./DevDetail b. Protection & Control > Details > DM Tree > Filter ./DevDetail/Ext c. Protection & Control > Details > DM Tree > Filter ./DevInfo d. Verify the hardware, software, firmware, IMEI, Manufacturer, Module Type are correctly reported for the module. 4. Verify that the detail for the custom MNO DevDetail nodes is reported correctly. The custom MNO DevDetail nodes supported by the module are listed in the Device Management IOT report. Following is the required list of custom MNO DevDetail nodes. The IOT report will confirm which ones are supported by the module. a. ./DevDetail/Ext/WLANMacAddr b. ./DevDetail/Ext/OrigFwV c. ./DevDetail/Ext/PreFwV d. ./DevDetail/Ext/InitActivationDate e. ./DevDetail/Ext/LastUpdateTime f. ./DevDetail/Ext/DownloadBearersUsed g. ./DevDetail/Ext/OSName h. ./DevDetail/Ext/OSVersion 5. Verify that the time stamps used for the Initial Activation Date and Last Update Time are in compliance with the Coordinated Universal Time UTC format.
Exit Criteria	1. The details are displayed on the server in the DM Tree (DevDetail and DevInfo) and are correct for the module. The details shall also include the custom MNO DevDetail nodes. 2. The module firmware version reported on the server is the same as displayed on the module. 3. The TAC code (first 6 digits of the IMEI) used by the module is the production TAC code (this TAC code will be included in the IMEI range for the launch/TA module hardware). 4. The other details reported for the module are correct (Hardware, Firmware, Software, IMEI). 5. The time stamps (Last Update Time and Initial Activation Date) are in compliance with Coordinated Universal Time UTC format: 6. Format: YYYY-MM-DDThh:mm:ssTZD where: a. YYYY = four-digit year b. MM = two-digit month (01=January, etc.) c. DD = two-digit day of month (01 through 31) d. hh = two digits of hour (00 through 23) (am/pm NOT allowed) e. mm = two digits of minute (00 through 59) f. ss = two digits of second (00 through 59)

TS35_5.2.5_TC_007

Purpose	Verify that the module in the host device reports the correct details to the server.
Requirement under test	TS.34_5.10_REQ_004, TS.34_5.10_REQ_004.1, TS.34_5.10_REQ_005, TS.34_5.10_REQ_005.1, TS.34_5.10_REQ_006, TS.34_5.10_REQ_006.1, TS.34_5.10_REQ_006.2, TS.34_5.10_REQ_006.3, TS.34_5.10_REQ_007, TS.34_5.10_REQ_007.1
Entry Criteria	1. Test case DHIR has been executed successfully. 2. Only a factory bootstrap account is provisioned on the module.
Test Procedure	1. Send a DM GET Check ALL to the module. 2. Look up the setting (./DevDetail/Ext/Host) value on the server in the following location: a. Protection & Control > Details > DM Tree > Filter ./DevDetail/Ext 3. Verify that the module settings are reported correctly: a. ./DevDetail/Ext/HostMan b. ./DevDetail/Ext/HostMod c. ./DevDetail/Ext/HostSwV d. ./DevDetail/Ext/HostPlasmaID e. ./DevDetail/Ext/IMEISV
Exit Criteria (Pass Criteria)	1. The module settings are reported correctly for the host device.

TS35_5.2.5_TC_008

Purpose	The purpose of this test is to verify that the module initiates a session with the DM server to report its new details after a FOTA update by a proprietary OEM server.
Requirement under test	TS.34_5.10_REQ_029, TS.34_5.10_REQ_029.1
Entry Criteria	1. Test case DHIR3 has been executed successfully. 2. Only a factory bootstrap account is provisioned on the module, and the module is configured on the server to use a factory bootstrap account. 3. The factory bootstrap account has been verified as a good bootstrap. 4. The module uses a proprietary update server to host the packages and does not use dual architecture with poke files (modules which don't apply shall have the test result marked as NA). 5. The module uses either OTA or side load method to update the firmware. 6. Module is configured on the MNO DM server.

Test Procedure	1. Execute an update on the module. 2. Module completes the download and update of the package hosted on the proprietary server. 3. Module automatically initiates a Device Initiated session with the MNO DM server to report the following new details after the update: a. Module IMEI b. Module Manufacturer c. Module Model Number d. ./DevDetail/Ext/HostMan e. ./DevDetail/Ext/HostMod f. ./DevDetail/Ext/HostSwV g. ./DevDetail/Ext/HostPlasmaID h. ./DevDetail/Ext/IMEISV 4. Verify that the time stamps used for the Initial Activation Date and Last Update Time are in compliance with the Coordinated Universal Time UTC format.
Exit Criteria	1. The module shall send a Device Initiated request to the DM server and report the new DevInfo details following the update. 2. The module processes the DM GET. 3. The details are displayed on the server in the DM Tree (DevDetail and DevInfo) and are correct for the module. This detail shall also include the custom MNO DevDetail nodes: a. IMEI b. Manufacturer c. Model Number d. ./DevDetail/Ext/HostMan e. ./DevDetail/Ext/HostMod f. ./DevDetail/Ext/HostSwV./DevDetail/Ext/HostPlasmaID 4. The time stamps (Last Update Time and Initial Activation Date) are in compliance with Coordinated Universal Time UTC format: a. Format: YYYY-MM-DDThh:mm:ssTZD where: i. YYYY = four-digit year ii. MM = two-digit month (01=January, etc.) iii. DD = two-digit day of month (01 through 31) iv. hh = two digits of hour (00 through 23) (am/pm NOT allowed) v. mm = two digits of minute (00 through 59) vi. ss = two digits of second (00 through 59) vii. TZD = time zone designator (Z or +hh:mm or -hh:mm)

TS35_5.2.5_TC_009

Purpose	The purpose of this test is to verify the module behaviour when it receives an update notification during a voice call.
Requirement under test	TS.34_5.10_REQ_024
Entry Criteria	1. Any update package listed in the 16038, with the exception of the corrupt package, can be used.
Test Procedure	1. Originate and accept a call from a land-line or other mobile phone. 2. The module is camped on the 2G, 3G, or LTE network. 3. During the call, initiate a NI update from the server. 4. Once both the call and download are complete, the module starts the update. 5. Complete the update.
Exit Criteria (Pass Criteria)	1. The module receives the server notification. 2. The Module Update session is successfully completed.

TS35_5.2.5_TC_010

Purpose	The purpose of this test is to verify that the module initiated update process is successful.
Requirement under test	DID28, DID30, DID31, DID32. TS.34_5.10_REQ_028, TS.34_5.10_REQ_030, TS.34_5.10_REQ_031, TS.34_5.10_REQ_032
Entry Criteria	1. Any update package listed in the 16038, with the exception of the corrupt package, can be used.
Test Procedure	1. Send an OMA DM GET command from the server to the module. 2. Initiate a user initiated update on the module. 3. Complete the download and update of the package on the module. 4. Send an OMA DM GET command from the server to the module.
Exit Criteria (Pass Criteria)	1. Module firmware version reported on the server matches the version displayed on the module. 2. User initiated request is displayed on the server. 3. User initiated update is successful for the module.

TS35_5.2.5_TC_011

Purpose	The purpose of this test is to verify that the default APN of the module is changed after sending a OMA DM REPLACE command to replace the APN as per the requirements of the MNO.
Requirement under test	TS.34_5.10_REQ_026, TS.34_5.10_REQ_026.1, TS.34_5.10_REQ_026.2, TS.34_5.10_REQ_026.3, TS.34_5.10_REQ_026.4

Entry Criteria	1. Test case TC-DHIR3 has been executed successfully. 2. Only a factory bootstrap account is provisioned on the module.
Test Procedure	1. Send a DM GET to the module to check existing APN. 2. Send an OMA DM REPLACE command to replace the APN. 3. Send a DM GET to the module to verify APN has changed. 4. Verify from the module side logs or AT command that the module used the designated APN when routing to the DM Server. 5. Power cycle the module. 6. Send a DM GET to the module to verify APN is correct. 7. Hard reset the module. 8. Send a DM GET to the module to verify APN is correct.
Exit Criteria (Pass Criteria)	1. DM GET is successful and APN does not change back upon executing a power cycle or hard reset. 2. Module side logs show the module used the designated APN to route to the MNO DM Server per the MNO requirements.

TS35_5.2.5_TC_012

Purpose	The purpose of this test is to verify that the default APN of the module is changed after sending a OMA DM ADD command to add a new default APN as per the requirements of the MNO.
Requirement under test	TS.34_5.10_REQ_027, TS.34_5.10_REQ_027.1, TS.34_5.10_REQ_027.2, TS.34_5.10_REQ_027.3, TS.34_5.10_REQ_027.4, TS.34_5.10_REQ_027.5, TS.34_5.10_REQ_027.6
Entry Criteria	1. Test case DHIR3 has been executed successfully. 2. Only a factory bootstrap account is provisioned on the module.
Test Procedure	1. Send a DM GET to the module to check existing APN. 2. Send an OMA DM ADD command to add an APN. 3. Send a DM GET to the module to verify APN has changed. 4. Verify from the module side logs or AT command that the module used the designated APN when routing to the DM Server. 5. Power cycle the module. 6. Send a DM GET to the module to verify APN is correct.
Exit Criteria (Pass Criteria)	1. DM GET is successful and APN does not change back upon executing a power cycle. 2. Module side logs show the module used the designated APN to route to the MNO DM Server per the MNO requirements.

TS35_5.2.5_TC_013

Purpose	The purpose of this test is to verify that the update process is successful after a hard reset of a DM 1.2 module.
Requirement under test	TS.34_5.10_REQ_014, TS.34_5.10_REQ_014.1
Entry Criteria	1. Test case DHIR3 has been executed successfully. 2. Only a factory bootstrap account is provisioned on the module. 3. Module client supports nonce resynchronization (this is mandatory for all DM 1.2 devices).
Test Procedure	1. Send an OMA DM GET command from the server to the module. 2. Initiate a NI update on the server for the module. 3. Complete the download and update of the package on the module. 4. Check the module firmware version reported on the server and displayed on the module. 5. Execute a hard reset on the module or re-flash the module. This action will reset the previously synchronized nonce value for client/server back to factory default on the client side. 6. Initiate a user initiated update on the module. 7. Complete the download and update of the package on the module. 8. Send an OMA DM GET command from the server to the module.
Exit Criteria (Pass Criteria)	1. Indication on server for a successful DM GET command. 2. NI Update request is displayed on the server. 3. NI Update is successful on the module. 4. Module firmware version reported on the server matches the version displayed on the module. 5. User initiated update is successful for the module. 6. User initiated request is displayed on the server. 7. User initiated update is successful for the module. 8. Indication on server for a successful DM GET command.

5.3 Void

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.

TS35_5.4_TC_001

Purpose	Default RPM Parameters are stored on Chipset when (U)SIM does not have RPM Parameters.
Requirement under test	TS.34_8.2.1_REQ_001, TS.34_8.2.1_REQ_007, TS.34_8.2.1_REQ_009, TS.34_8.2.4_REQ_010
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 TS.34_8.2.4_REQ_010.

TS35_5.4_TC_002

Purpose	RPM Activation Control - RPM Parameters are present on (U)SIM.
Requirement under test	TS.34_8.2.1_REQ_002, TS.34_8.2.1_REQ_002.1, TS.34_8.2.1_REQ_007, TS.34_8.2.1_REQ_008
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 TS.34_8.2.4_REQ_010.
(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.

TS35_5.4_TC_003

Purpose	RPM Activation Control – When RPM Parameters are Not Present in (U)SIM
Requirement under test	TS.34_8.2.1_REQ_003, TS.34_8.2.1_REQ_007, TS.34_8.2.1_REQ_009
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.

TS35_5.4_TC_004

Purpose	RPM is enabled when IoT Device is roaming.
Requirement under test	TS.34_8.2.1_REQ_004
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 after step 3. 5. Verify IoT Device resets after time T1 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 after step 6. 8. Verify IoT Device resets after time T1 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.

TS35_5.4_TC_005

Void

TS35_5.4_TC_005a

Purpose	RPM can be disabled through SIM OTA.

Requirement under test	TS.34_8.2.1_REQ_005, TS.34_8.2.4_REQ_009, TS.34_8.2.4_REQ_009.1, TS.34_8.2.4_REQ_009.2
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.

TS35_5.4_TC_005b

Purpose	A single RPM requirement can be disabled through SIM OTA.
Requirement under test	TS.34_8.2.1_REQ_005, TS.34_8.2.2_REQ_008, TS.34_8.2.4_REQ_009, TS.34_8.2.4_REQ_009.1, TS.34_8.2.4_REQ_009.2
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.

TS35_5.4_TC_005c

Purpose	Verify RPM is disabled when RPM_Enabled_Flag is OFF on (U)SIM card.
Requirement under test	TS.34_8.2.1_REQ_005, TS.34_8.2.4_REQ_009, TS.34_8.2.4_REQ_009.1, TS.34_8.2.4_REQ_009.2
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) (U)SIM-RPM03 (See annex A)
Test Procedure	1. Verify, that USIM settings are in line with (U)SIM-RPM01 2. Switch ON the IoT Device. 3. Verify RPM is enabled. 4. Set RPM_Enabled_Flag to OFF on SIM card. For this, switch off the device, write parameter settings (U)SIM-RPM03 to the USIM and switch on the device again 5. Verify RPM is disabled.
Exit Criteria	1. Verify RPM is enabled / disabled on the device as per the (U)SIM flag.

TS35_5.4_TC_006

Purpose	Verify "RPM Version Implemented" file on (U)SIM card is updated with the correct RPM version.
Requirement under test	TS.34_8.2.1_REQ_006, TS.34_8.2.1_REQ_006.1, TS.34_8.2.1_REQ_006.2, TS.34_8.2.1_REQ_006.3
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.

TS35_5.4_TC_007

Purpose	Verify that RPM operation management counters are reset after RPM parameters are updated through OTA.
Requirement under test	TS.34_8.2.2_REQ_002
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.

TS35_5.4_TC_008

Void

TS35_5.4_TC_008a

Purpose	RPM controls number of SW resets when LU/Attach is rejected with permanent MM/GMM cause.
Requirement under test	TS.34_8.2.2_REQ_003, TS.34_8.2.2_REQ_003.1, TS.34_8.2.2_REQ_004, TS.34_8.2.2_REQ_004.1 TS.34_8.2.2_REQ_005, TS.34_8.2.2_REQ_005.1
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 receives a maximum of (N1 + 1) registration attempts in step 3. Note: The +1 is to account for registration attempt following T1 as expiry per the note in requirement TS.34_8.2.2_REQ_003. 2. Verify RPM increments counter C-BR-1 by N1. 3. Verify registration is triggered for the reset in step 5.

TS35_5.4_TC_008b

Purpose	RPM controls number of SW resets when Attach is rejected with permanent EMM cause.
Requirement under test	TS.34_8.2.2_REQ_003, TS.34_8.2.2_REQ_003.1, TS.34_8.2.2_REQ_004, TS.34_8.2.2_REQ_004.1
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 receives a maximum of (N1 + 1) Attach Requests in step 3. Note: The +1 is to account for registration attempt following T1 expiry as per the note in requirement TS.34_8.2.2_REQ_003.

TS35_5.4_TC_008c

Purpose	Verify that RPM does not control the number of SW resets when N1 is set to 0.
Requirement under test	TS.34_8.2.2_REQ_003, TS.34_8.2.2_REQ_003.1
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

TS35_5.4_TC_009

Void

TS35_5.4_TC_009a

Purpose	RPM waits for time T1 and resets the modem after permanent MM/GMM reject.
Requirement under test	TS.34_8.2.2_REQ_006, TS.34_8.2.2_REQ_006.1, TS.34_8.2.2_REQ_006.2, TS.34_8.2.2_REQ_007, TS.34_8.2.2_REQ_007.1, TS.34_8.2.4_REQ_001
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 after step 4. 2. Verify IoT Device attempts LU/Attach after T1 expires. 3. Verify RPM increments counter C-R-1 by 1.

TS35_5.4_TC_009b

Purpose	RPM waits for time T1 and resets the modem after permanent GMM reject.
Requirement under test	TS.34_8.2.2_REQ_006, TS.34_8.2.2_REQ_006.1, TS.34_8.2.2_REQ_006.2, TS.34_8.2.2_REQ_007, TS.34_8.2.2_REQ_007.1, TS.34_8.2.4_REQ_001
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 after step 4. 2. Verify IoT Device attempts LU/Attach after T1 expires. 3. Verify IoT Device increments counter C-R-1 by 1.

TS35_5.4_TC_009c

Purpose	RPM waits for time T1 and resets the modem after permanent EMM reject.
Requirement under test	TS.34_8.2.2_REQ_006, TS.34_8.2.2_REQ_006.1, TS.34_8.2.2_REQ_006.2, TS.34_8.2.2_REQ_007, TS.34_8.2.2_REQ_007.1, TS.34_8.2.4_REQ_001
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. Wait for 'Attach Request' from IoT Device/ IoT communication module. 3. SS sends Attach Request Reject with a Permanent Mobility EMM reject cause listed in TS.34_8.2.2_REQ_006 4. SS listens for connection requests for at least T1 period. 5. Repeat steps 2 to 4 for each remaining EMM reject cause listed in TS.34_8.2.2_REQ_006
Exit Criteria	1. Verify IoT Device does not send Attach before T1 after step 4. 2. Verify IoT Device attempts Attach after T1 expires. 3. Verify IoT Device increments counter C-R-1 by 1.

TS35_5.4_TC_010

Purpose	Service requests will not trigger additional registration attempts.
Requirement under test	TS.34_8.2.2_REQ_009
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.

TS35_5.4_TC_011

Purpose	Service requests will not trigger additional registration attempts.
Requirement under test	TS.34_8.2.2_REQ_010
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.

TS35_5.4_TC_012

Purpose	RPM controls # of PDP context activation requests in PDP ignore scenario.
Requirement under test	TS.34_8.2.3_REQ_001, TS.34_8.2.3_REQ_002, TS.34_8.2.3_REQ_002.1, TS.34_8.2.3_REQ_007
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.

TS35_5.4_TC_013

Purpose	RPM controls # of PDP context activation requests in "permanent" PDP reject scenario.
Requirement under test	TS.34_8.2.3_REQ_003, TS.34_8.2.3_REQ_003.1, TS.34_8.2.3_REQ_004, TS.34_8.2.3_REQ_004.1, TS.34_8.2.3_REQ_007
Entry Criteria	1. IoT communication module supports RPM feature.
(U)SIM Parameter Settings	(U)SIM-RPM01 (See annex A) Set SM_RetryWaitTime value to 0 sec in USIM (see TS 31.102 clause 4.2.94 [3])
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 a SM reject cause listed in TS.34_8.2.3_REQ_003 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 Iall PDP requests received from IoT Device are rejected by SS with the SM reject cause selected from the list in TS.34_8.2.3_REQ_003. 5. Repeat steps 2 to 4 for each remaining SM reject cause listed in TS.34_8.2.3_REQ_003
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 C-PDP-2 counter is incremented each time the PDP Context Activation Request is ignored.

TS35_5.4_TC_014

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	TS.34_8.2.3_REQ_005, TS.34_8.2.3_REQ_005.1, TS.34_8.2.3_REQ_006, TS.34_8.2.3_REQ_006.1, TS.34_8.2.3_REQ_007

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. IoT Device sends PDP Context Activation Request, which is rejected by SS by the SM reject cause selected from the list TS.34_8.2.3_REQ_005 . 4. SS Issues 2xF3 PDP Activation Requests to the same APN in an hour (evenly distributed) and all PDP requests received from IoT Device are rejected by SS with SM reject cause selected from the list in TS.34_8.2.3_REQ_005by the network. 5. Repeat steps 2 to 4 for each remaining SM reject cause listed in TS.34_8.2.3_REQ_005
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

TS35_5.4_TC_015

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	TS.34_8.2.3_REQ_008, TS.34_8.2.3_REQ_008.1, TS.34_8.2.3_REQ_008.2 TS.34_8.2.3_REQ_009, TS.34_8.2.3_REQ_009.1
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.

TS35_5.4_TC_016

Purpose	Verify the periodic Decrement of RPM operation management counters.
Requirement under test	TS.34_8.2.4_REQ_004, TS.34_8.2.4_REQ_004.1, TS.34_8.2.4_REQ_004.2, TS.34_8.2.4_REQ_005, TS.34_8.2.4_REQ_005.1, TS.34_8.2.4_REQ_005.2, TS.34_8.2.4_REQ_006, TS.34_8.2.4_REQ_006.1, TS.34_8.2.4_REQ_006.2
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.

TS35_5.4_TC_017

Purpose	Verify "EF-RPM Operational Management Counters" can be read through OTA
Requirement under test	TS.34_8.2.4_REQ_007

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;

TS35_5.4_TC_018

Purpose	Verify RPM (U)SIM Parameters
Requirement under test	TS.34_8.2.4_REQ_008
Entry Criteria	1. (U)SIM supports RPM feature
(U)SIM Parameter Settings	(U)SIM-RPM06 (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 – 3F00/ 7F66/5F40/4F42 e. EF-RPM Operational Management Counters - 3F00/7F66/5F40/4F43 f. EF-RPM Version Information 3F00/7F66/5F40/4F44

TS35_5.4_TC_019

Purpose	RPM correctly controls number of SW retries according to 3GPP and no reset occurs when Attach is rejected with temporary Mobility Management cause.
Requirement under test	TS.34_8.2.2_REQ_011
Entry Criteria	IoT Device application supports RPM features.
(U)SIM Parameter Settings	(U)SIM-RPM02 (See annex A)
Test Procedure	1. Activate the cell. 2. Power ON IoT Device.

	3. SS sends Attach Request Reject with a Mobility Management cause listed in TS.34_8.2.2_REQ_011 4. IoT Device retries Attach Request according to the behaviour described in TS.34_8.2.2_REQ_011for the reject cause 5. Confirm that at no time the IoT device resets after recieving any reject cause 6. Repeat steps 3 to 5 for each Reject cause listed in TS.34_8.2.2_REQ_011 7. Power OFF IoT Device.
Exit Criteria	Verify that the IoT device sends up to the maximum number of retries according to the behaviour in Refences TS.34_8.2.2_REQ_011 for each reject cause No resets occur during any Attach Requests

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 Test Applicability and Classification

- “x” - This test case can be run in this test environment.
- “o” - It is not possible to execute the test case in this test environment.
- “xo” - This test case can partly be run in this test environment.

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
3	IoT Device Requirements	TS.34_3.0_REQ_001	-	High level requirement.					
		TS.34_3.0_REQ_002	-	High level requirement.					
		TS.34_3.0_REQ_003	-	See GSMA TS.24 [2].					
		TS.34_3.0_REQ_004	-	High level requirement.					
4	IoT Device Application Requirements	TS.34_4.0_REQ_001	TS35_5.1_TC_001		x	x	x	x	All test environments are possible + IOT Platform needed

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_4.0_REQ_002	TS35_5.1_TC_002		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_003	TS35_5.1_TC_003		x	o	x	x	Only one device can be monitored at a time in Simulated environment
		TS.34_4.0_REQ_004	-	For future study					
		TS.34_4.0_REQ_005	TS35_5.1_TC_004a		o	x	o	o	No Mobile Network (controlled, simulated or live) needed at all
		TS.34_4.0_REQ_005	TS35_5.1_TC_004b		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_006 TS.34_4.0_REQ_006.1	TS35_5.1_TC_005		x	x	x	x	All test environments are

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_4.0_REQ_006.2							possible + IOT Platform needed
		TS.34_4.0_REQ_007	TS35_5.1_TC_006		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_008	TS35_5.1_TC_007		x	x	o	x	IOT Platform needed
		TS.34_4.0_REQ_009	TS35_5.1_TC_007		x	x	o	x	IOT Platform needed
		TS.34_4.0_REQ_010	-	For future study					
		TS.34_4.0_REQ_011 TS.34_4.0_REQ_011.1 TS.34_4.0_REQ_011.2	TS35_5.1_TC_008a		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_011 TS.34_4.0_REQ_011.1 TS.34_4.0_REQ_011.2	TS35_5.1_TC_008b		x	x	x	x	All test environments are possible + IOT Platform needed

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_4.0_REQ_011 TS.34_4.0_REQ_011.1 TS.34_4.0_REQ_011.2	TS35_5.1_TC_008c		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_011 TS.34_4.0_REQ_011.1 TS.34_4.0_REQ_011.2	TS35_5.1_TC_008d		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_011 TS.34_4.0_REQ_011.1 TS.34_4.0_REQ_011.2	TS35_5.1_TC_008e		x	x	o	x	IOT Platform needed
		TS.34_4.0_REQ_011 TS.34_4.0_REQ_011.1 TS.34_4.0_REQ_011.2	TS35_5.1_TC_008f		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_011 TS.34_4.0_REQ_011.1 TS.34_4.0_REQ_011.2	TS35_5.1_TC_008g		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_011 TS.34_4.0_REQ_011.1	TS35_5.1_TC_008h		x	x	x	x	All test environments are

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_4.0_REQ_011.2							possible + IOT Platform needed
		TS.34_4.0_REQ_011 TS.34_4.0_REQ_011.1 TS.34_4.0_REQ_011.2	TS35_5.1_TC_008i		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_012 TS.34_4.0_REQ_012.1 TS.34_4.0_REQ_012.2 TS.34_4.0_REQ_012.3	TS35_5.1_TC_009		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_013 TS.34_4.0_REQ_013.1 TS.34_4.0_REQ_013.2 TS.34_4.0_REQ_013.3	TS35_5.1_TC_010		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_014 TS.34_4.0_REQ_014.1	TS35_5.1_TC_011		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_015	-	For future study					

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_4.0_REQ_016	TS35_5.1_TC_012		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_017	-	For future study					
		TS.34_4.0_REQ_018	-	For future study					
		TS.34_4.0_REQ_019	TS35_5.1_TC_013		x	x	x	x	All test environments are possible
		TS.34_4.0_REQ_020	TS35_5.1_TC_014		o	x	x	x	IOT Platform needed
		TS.34_4.0_REQ_021	TS35_5.1_TC_015a		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_021	TS35_5.1_TC_015b		x	x	x	x	All test environments are possible + IOT Platform needed

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_4.0_REQ_022 TS.34_4.0_REQ_022.1	TS35_5.1_TC_016a		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_022 TS.34_4.0_REQ_022.1	TS35_5.1_TC_016b		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_023	-						
		TS.34_4.0_REQ_024	TS35_5.1_TC_017		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_025	TS35_5.1_TC_018		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_4.0_REQ_026	-	For future study					
		TS.34_4.0_REQ_027	-	For future study					

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_4.0_REQ_028	-	For future study					
		TS.34_4.0_REQ_029 TS.34_4.0_REQ_029.1	-	For future study					
5.1	Standards Compliance	TS.34_5.1_REQ_001	-	Out of scope					
		TS.34_5.1_REQ_002	-	Out of scope					
		TS.34_5.1_REQ_003	-	Out of scope					
5.2	Network Efficiency Requirements	TS.34_5.2_REQ_001	-	High level requirement					
		TS.34_5.2_REQ_002	-	For future study					
		TS.34_5.2_REQ_003	-	Out of scope					
5.3	Requirements for Communication Modules that Support IPv6	TS.34_5.3_REQ_001	TS35_5.2.1_TC_001		o	x	x		Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_5.3_REQ_002	TS35_5.2.1_TC_002		o	x	x		Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_5.3_REQ_003	TS35_5.2.1_TC_003		o	x	x		Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_5.3_REQ_004	TS35_5.2.1_TC_004		o	x	x		Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_5.3_REQ_005	TS35_5.2.1_TC_005		o	x	x		Simulated mobile network environment (i.e. a 3GPP protocol test

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
									instrument in a test lab)
5.4	Requirements for Communication Modules that Support LTE	TS.34_5.4_REQ_001	-	Out of scope					
5.5	Requirements for Communication Modules that Support Fast Dormancy	TS.34_5.5_REQ_001	TS35_5.2.2_TC_001		x	x	x		All test environments are possible
		TS.34_5.5_REQ_002	-	For future study					
5.6	(U)SIM Interface Requirements	TS.34_5.6_REQ_001	-	Out of scope					
		TS.34_5.6_REQ_002	-	Out of scope					
5.7	Security Requirements	TS.34_5.7_REQ_001	-	High level requirement					

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_5.7_REQ_002 TS.34_5.7_REQ_002.1	TS35_5.2.3_TC_001		x	x	x	o	All test environments are possible
		TS.34_5.7_REQ_003	-	For future study					
		TS.34_5.7_REQ_004	TS35_5.2.3_TC_002		x	x	x	o	All test environments are possible
		TS.34_5.7_REQ_005	-	For future study					
5.8	Device Management	TS.34_5.8_REQ_001	-	High level requirement					
		TS.34_5.8_REQ_002	-	High level requirement					
		TS.34_5.8_REQ_003	TS35_5.1_TC_017		x	x	x	x	All test environments are possible + IOT Platform needed
		TS.34_5.8_REQ_004	TS35_5.1_TC_018		x	x	x	x	All test environments are

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
									possible + IOT Platform needed
5.9	Subscription Identifier Requirements	TS.34_5.9_REQ_001	TS35_5.2.4_TC_001		x	x	x	o	This can be tested with or without network.
		TS.34_5.9_REQ_002	TS35_5.2.4_TC_002		x	x	x	o	This can be tested with or without network.
5.10	Device Host Identity Reporting								
		TS.34_5.10_REQ_001	TS35_5.2.5_TC_001 TS35_5.2.5_TC_003						
		TS.34_5.10_REQ_002 TS.34_5.10_REQ_002.1	TS35_5.2.5_TC_002						
		TS.34_5.10_REQ_003 TS.34_5.10_REQ_003.1 TS.34_5.10_REQ_003.2	TS35_5.2.5_TC_002						
		TS.34_5.10_REQ_004 TS.34_5.10_REQ_004.1	TS35_5.2.5_TC_007						

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_5.10_REQ_005 TS.34_5.10_REQ_005.1	TS35_5.2.5_TC_007						
		TS.34_5.10_REQ_006 TS.34_5.10_REQ_006.1 TS.34_5.10_REQ_006.2 TS.34_5.10_REQ_006.3	TS35_5.2.5_TC_007						
		TS.34_5.10_REQ_007 TS.34_5.10_REQ_007.1	TS35_5.2.5_TC_007						
		TS.34_5.10_REQ_008	For future study						
		TS.34_5.10_REQ_009	For future study						
		TS.34_5.10_REQ_010 TS.34_5.10_REQ_010.1	For future study						
		TS.34_5.10_REQ_011 TS.34_5.10_REQ_011.1	For future study						
		TS.34_5.10_REQ_012	For future study						
		TS.34_5.10_REQ_013 TS.34_5.10_REQ_013.1	For future study						

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_5.10_REQ_015	For future study						
		TS.34_5.10_REQ_016	For future study						
		TS.34_5.10_REQ_017	For future study						
		TS.34_5.10_REQ_018	For future study						
		TS.34_5.10_REQ_019	For future study						
		TS.34_5.10_REQ_020	For future study						
		TS.34_5.10_REQ_021	For future study						
		TS.34_5.10_REQ_022	TS35_5.2.5_TC_006						
		TS.34_5.10_REQ_023	TS35_5.2.5_TC_006						
		TS.34_5.10_REQ_024	TS35_5.2.5_TC_009						
		TS.34_5.10_REQ_025 TS.34_5.10_REQ_025.1	TS35_5.2.5_TC_006						
		TS.34_5.10_REQ_026 TS.34_5.10_REQ_026.1	TS35_5.2.5_TC_011						

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_5.10_REQ_026.2 TS.34_5.10_REQ_026.3 TS.34_5.10_REQ_026.4							
		TS.34_5.10_REQ_027 TS.34_5.10_REQ_027.1 TS.34_5.10_REQ_027.2 TS.34_5.10_REQ_027.3 TS.34_5.10_REQ_027.4 TS.34_5.10_REQ_027.5 TS.34_5.10_REQ_027.6	TS35_5.2.5_TC_012						
		TS.34_5.10_REQ_028	TS35_5.2.5_TC_010						
		TS.34_5.10_REQ_029 TS.34_5.10_REQ_029.1	TS35_5.2.5_TC_010						
		TS.34_5.10_REQ_030	TS35_5.2.5_TC_010						
		TS.34_5.10_REQ_031	TS35_5.2.5_TC_010						
		TS.34_5.10_REQ_032	TS35_5.2.5_TC_010						
		TS.34_5.10_REQ_033	TS35_5.2.5_TC_004						

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
5.11	Communication Modules that Support 5G	TS.34_5.11_REQ_001	For future study						
6	IoT Service Provider Requirements	TS.34_6.0_REQ_001	-	For future study					
		TS.34_6.0_REQ_002 TS.34_6.0_REQ_002.1 TS.34_6.0_REQ_002.2	-	Out of scope					
		TS.34_6.0_REQ_003	-	For future study					
		TS.34_6.0_REQ_004	-	For future study					
		TS.34_6.0_REQ_005 TS.34_6.0_REQ_005.1	-	For future study					
7	Policy Based Connection Efficiency Requirements								

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
7.2.1	Network Friendly Mode General Mechanism	TS.34_7.2.1_REQ_001	-TS35_5.3_TC_001	For future study					
		TS.34_7.2.1_REQ_002	-TS35_5.3_TC_002	For future study					
		TS.34_7.2.1_REQ_003	--	For future study High level requirement.					
7.2.2 7.5	Policy Management IoT Device Action Linked to Cause Code	TS.34_7.2.2 _REQ_001TS.34_5.2_REQ_001	-TS35_5.3_TC_020	For future study	x	x	x	o	All test environments are possible
		TS.34_7.02.2_REQ_002	-	For future studyHigh level requirement.					
8.2.1	Radio Policy Manager - General	TS.34_8.2.1_REQ_001	TS35_5.3_TC_020		x	x	x	o	All test environments are possible

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_8.2.1_REQ_002 TS.34_8.2.1_REQ_002.1	TS35_5.4_TC_002		x	x	x	o	All test environments are possible
		TS.34_8.2.1_REQ_003	TS35_5.4_TC_003		x	x	x	o	All test environments are possible
		TS.34_8.2.1_REQ_004	TS35_5.4_TC_004		o	x	o	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab) is needed
		TS.34_8.2.1_REQ_005	TS35_5.4_TC_005a		o	x	o	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab) is needed
		TS.34_8.2.1_REQ_005	TS35_5.4_TC_005b		o	x	o	o	Simulated mobile network environment (i.e. a 3GPP protocol test

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
									instrument in a test lab) is needed
		TS.34_8.2.1_REQ_005	TS35_5.4_TC_005c		o	x	o	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab) is needed
		TS.34_8.2.1_REQ_006 TS.34_8.2.1_REQ_006.1 TS.34_8.2.1_REQ_006.2 TS.34_8.2.1_REQ_006.3	TS35_5.4_TC_006		x	x	x	o	All test environments are possible
8.2.2	Radio Policy Manager - Mobility Management	TS.34_8.2.2_REQ_001	-	High level requirement.					
		TS.34_8.2.2_REQ_002	TS35_5.4_TC_007		x	x	x	o	All test environments are possible
		TS.34_8.2.2_REQ_003 TS.34_8.2.2_REQ_003.1	TS35_5.4_TC_008a		x	x	x	o	Simulated mobile network environment (i.e. a

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
									3GPP protocol test instrument in a test lab)
		TS.34_8.2.2_REQ_003 TS.34_8.2.2_REQ_003.1	TS35_5.4_TC_008b		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.2_REQ_003 TS.34_8.2.2_REQ_003.1	TS35_5.4_TC_008c		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.2_REQ_004 TS.34_8.2.2_REQ_004.1	TS35_5.4_TC_008a		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_8.2.2_REQ_004 TS.34_8.2.2_REQ_004.1	TS35_5.4_TC_008b		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.2_REQ_005 TS.34_8.2.2_REQ_005.1	TS35_5.4_TC_008a		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.2_REQ_006 TS.34_8.2.2_REQ_006.1 TS.34_8.2.2_REQ_006.2	TS35_5.4_TC_009a		o	x	o	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.2_REQ_006 TS.34_8.2.2_REQ_006.1 TS.34_8.2.2_REQ_006.2	TS35_5.4_TC_009b		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
									instrument in a test lab)
		TS.34_8.2.2_REQ_006 TS.34_8.2.2_REQ_006.1 TS.34_8.2.2_REQ_006.2	TS35_5.4_TC_009c		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.2_REQ_007 TS.34_8.2.2_REQ_007.1	TS35_5.4_TC_009a		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.2_REQ_007 TS.34_8.2.2_REQ_007.1	TS35_5.4_TC_009b		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.2_REQ_007 TS.34_8.2.2_REQ_007.1	TS35_5.4_TC_009c		x	x	x	o	Simulated mobile network

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
									environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.2_REQ_008	-	For future study					
		TS.34_8.2.2_REQ_009	TS35_5.4_TC_010		o	x	o	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.2_REQ_010	TS35_5.4_TC_011		o	x	o	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.2_REQ_011	TS35_5.4_TC_019		o	x	o	o	Simulated mobile network environment (i.e. a 3GPP protocol test

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
									instrument in a test lab)
8.2.3	Radio Policy Manager – Session Management	TS.34_8.2.3_REQ_001	TS35_5.4_TC_012		o	x	o	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.3_REQ_002 TS.34_8.2.3_REQ_002.1	TS35_5.4_TC_012		o	x	o	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.3_REQ_003 TS.34_8.2.3_REQ_003.1	TS35_5.4_TC_013		xo	x	xo	o	Partly covered in live network and Controlled Mobile Network depending on each network and user equipment capabilities

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_8.2.3_REQ_004 TS.34_8.2.3_REQ_004.1	TS35_5.4_TC_013		o	x	o	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.3_REQ_005 TS.34_8.2.3_REQ_005.1	TS35_5.4_TC_013		xo	x	xo	o	Partly covered in live network and Controlled Mobile Network depending on each network and user equipment capabilities
		TS.34_8.2.3_REQ_006 TS.34_8.2.3_REQ_006.1	TS35_5.4_TC_013		o	x	o	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.3_REQ_007	TS35_5.4_TC_012		o	x	o	o	Simulated mobile network environment (i.e. a

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
									3GPP protocol test instrument in a test lab)
		TS.34_8.2.3_REQ_007	TS35_5.4_TC_013		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.3_REQ_007	TS35_5.4_TC_014		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.3_REQ_008	TS35_5.4_TC_015		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_8.2.3_REQ_009	TS35_5.4_TC_015		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
8.2.4	Timers and Counters	TS.34_8.2.4_REQ_001	TS35_5.4_TC_009a		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.4_REQ_001	TS35_5.4_TC_009b		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test instrument in a test lab)
		TS.34_8.2.4_REQ_001	TS35_5.4_TC_009c		x	x	x	o	Simulated mobile network environment (i.e. a 3GPP protocol test

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
									instrument in a test lab)
		TS.34_8.2.4_REQ_002	-	For future study					
		TS.34_8.2.4_REQ_003 TS.34_8.2.4_REQ_003.1	-	For future study					
		TS.34_8.2.4_REQ_004 TS.34_8.2.4_REQ_004.1 TS.34_8.2.4_REQ_004.2	TS35_5.4_TC_016		x	x	x	o	All test environments are possible
		TS.34_8.2.4_REQ_005 TS.34_8.2.4_REQ_005.1 TS.34_8.2.4_REQ_005.2	TS35_5.4_TC_016		x	x	x	o	All test environments are possible
		TS.34_8.2.4_REQ_006 TS.34_8.2.4_REQ_006.1 TS.34_8.2.4_REQ_006.2	TS35_5.4_TC_016		x	x	x	o	All test environments are possible
		TS.34_8.2.4_REQ_007	TS35_5.4_TC_017		x	x	x	o	All test environments are possible

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
		TS.34_8.2.4_REQ_008	TS35_5.4_TC_018		x	x	x	o	All test environments are possible
		TS.34_8.2.4_REQ_009 TS.34_8.2.4_REQ_009.1 TS.34_8.2.4_REQ_009.2	TS35_5.4_TC_005a		x	x	x	x	Logging is needed and OTA capability in the IOT platform
		TS.34_8.2.4_REQ_009 TS.34_8.2.4_REQ_009.1 TS.34_8.2.4_REQ_009.2	TS35_5.4_TC_005b		x	x	x	x	Logging is needed and OTA capability in the IOT platform
		TS.34_8.2.4_REQ_009 TS.34_8.2.4_REQ_009.1 TS.34_8.2.4_REQ_009.2	TTS35_5.4_TC_005c		x	x	x	x	Logging is needed and OTA capability in the IOT platform
		TS.34_8.2.4_REQ_010	TS35_5.4_TC_001		x	x	x	o	All test environments are possible
9.1	Rejection of IoT Device Requests with Back-off Timer		-	See associated GCF or PTCRB test cases.					

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
9.2	Handling of Low Access Priority Indicator		-	See associated GCF or PTCRB test cases.					
9.3	Implicit Reject in GSM Radio Network		-	See associated GCF or PTCRB test cases.					
9.4	Long Periodic LAU/RAU/TAU		-	See associated GCF or PTCRB test cases.					
9.5	Extended Access Barring		-	See associated GCF or PTCRB test cases.					
9.6	Extended NMO-I		-	See associated					

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
				GCF or PTCRB test cases.					
9.7	Minimum Periodic Search Timer		-	See associated GCF or PTCRB test cases.					
9.8	Attach with IMSI Indicator		-	See associated GCF or PTCRB test cases.					
9.9	Timer T3245		-	See associated GCF or PTCRB test cases.					
9.10	Configuration of 3GPP Release 10 Connection		-	See associated GCF or					

Section	IoT Device Connection Efficiency Guidelines Section	Requirement	Test Case	Comments	3.1 Controlled Mobile Network	3.2 Simulated Mobile Network	3.3 Live Mobile Network	IoT Platform Needed	Test Environment classification
	Efficiency Parameters			PTCRB test cases.					
9.11	Power Saving Mode		-	See associated GCF or PTCRB test cases.					

Annex C Test Applicability and Classification for certification Organisations.

This annex provides additional information which can be used by certification organisations.

1) Applicability for module and product integrating a module.

As per specified in the TS.34 section 2.1 (figure below) an IoT Device can re-use a Communication module. In the following this type of IoT Device is called “IoT Device integrating a module”

When the Communication Module has been certified it is not necessary to re-run some of the TCs for the IoT Device integrating the certified module.

The applicable test cases for the certification for modules and IoT Device integrating a module are listed in the table below.

Entities	TS.34 Section	TS.35 sections	Module	Module with Service Layer	IoT Device integrating a module
Application	4.0/4.1	5.1			X
Service Layer	4.2	5.1 (partly)		X	
Communication Module	5/7/8/9	5.2/5.3/5.4	X	X	

2) Applicability depending on the supported technology.

The RPM test cases used for the device certification are applicable depending on the device technology supported by the IoT device as per below

TS.34 chapter	Features	Requirements	TS.35 TCs	GSM	UMTS	LTE
8.2.1	Radio Policy Manager - General	TS.34_8.2.1_REQ_001	TS.35_5.4_TC_001	X	X	X
		TS.34_8.2.1_REQ_002	TS.35_5.4_TC_002	X	X	X
		TS.34_8.2.1_REQ_003	TS.35_5.4_TC_003	X	X	X
		TS.34_8.2.1_REQ_004	TS.35_5.4_TC_004	X	X	
		TS.34_8.2.1_REQ_005	TS.35_5.4_TC_005a	X	X	
			TS.35_5.4_TC_005b	X	X	
			TS.35_5.4_TC_005c	X	X	X
		TS.34_8.2.1_REQ_006	TS.35_5.4_TC_006	X	X	

TS.34 chapter	Features	Requirements	TS.35 TCs	GSM	UMTS	LTE
8.2.2	Radio Policy Manager - Mobility Management	TS.34_8.2.2_REQ_001				
		TS.34_8.2.2_REQ_002	TS.35_5.4_TC_007	X	X	
		TS.34_8.2.2_REQ_003	TS.35_5.4_TC_008a	X	X	
			TS.35_5.4_TC_008b			X
			TS.35_5.4_TC_008c	X	X	X
		TS.34_8.2.2_REQ_004	TS.35_5.4_TC_008a	X	X	
			TS.35_5.4_TC_008b			X
		TS.34_8.2.2_REQ_005	TS.35_5.4_TC_008a	X	X	
		TS.34_8.2.2_REQ_006	TS.35_5.4_TC_009a	X	X	
			TS.35_5.4_TC_009b	X	X	
			TS.35_5.4_TC_009c			X
		TS.34_8.2.2_REQ_007	TS.35_5.4_TC_009a	X	X	
			TS.35_5.4_TC_009b	X	X	
			TS.35_5.4_TC_009c			X
		TS.34_8.2.2_REQ_008	TS.35_5.4_TC_005b	X	X	
		TS.34_8.2.2_REQ_009	TS.35_5.4_TC_010	X	X	
		TS.34_8.2.2_REQ_010	TS.35_5.4_TC_011	X	X	
		TS.34_8.2.2_REQ_011	TS35_5.4_TC_019	X	X	X
8.2.3	Radio Policy Manager – Session Management	TS.34_8.2.3_REQ_001	TS.35_5.4_TC_012	X	X	
		TS.34_8.2.3_REQ_002	TS.35_5.4_TC_012	X	X	
		TS.34_8.2.3_REQ_003	TS.35_5.4_TC_013	X	X	
		TS.34_8.2.3_REQ_004	TS.35_5.4_TC_013	X	X	
		TS.34_8.2.3_REQ_005	TS.35_5.4_TC_014	X	X	
		TS.34_8.2.3_REQ_006	TS35_5.4_TC_014	X	X	
		TS.34_8.2.3_REQ_007	TS.35_5.4_TC_012	X	X	
			TS.35_5.4_TC_013	X	X	
			TS.35_5.4_TC_014	X	X	
		TS.34_8.2.3_REQ_008	TS.35_5.4_TC_015	X	X	
		TS.34_8.2.3_REQ_009	TS.35_5.4_TC_015	X	X	
8.2.4	Timers and Counters	TS.34_8.2.4_REQ_001	TS.35_5.4_TC_009a	X	X	
			TS.35_5.4_TC_009b	X	X	
			TS.35_5.4_TC_009c			X
		TS.34_8.2.4_REQ_002	-			
		TS.34_8.2.4_REQ_003	-			
		TS.34_8.2.4_REQ_004	TS.35_5.4_TC_016	X	X	X
		TS.34_8.2.4_REQ_005	TS.35_5.4_TC_016	X	X	X
		TS.34_8.2.4_REQ_006	TS.35_5.4_TC_016	X	X	X
		TS.34_8.2.4_REQ_007	TS.35_5.4_TC_017	X	X	

TS.34 chapter	Features	Requirements	TS.35 TCs	GSM	UMTS	LTE
		TS.34_8.2.4_REQ_008	TS.35_5.4_TC_018	X	X	X
		TS.34_8.2.4_REQ_009	TS.35_5.4_TC_005a	X	X	
			TS.35_5.4_TC_005b	X	X	
			TS.35_5.4_TC_005c	X	X	X
		TS.34_8.2.4_REQ_010	TS.35_5.4_TC_001	X	X	X

Annex D Document Management

D.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
2.0	01 July 2015	Test cases for DHIR added in section 5.2.5, Updated test environments descriptions in section 3, Test Applicability and Classification added in Annex B. Minor editorial updates.	CLP/PSMC	Ian Smith/GSMA Jerome Hamel / 7Layers
	01 July 2015	Change of ownership to GSMA TSG and the document re-numbered to TS.35	TSG	Jerome Hamel / 7Layers
3.0	Jan 2016	Test Cases re-numbered	TSG	Jerome Hamel / 7Layers
4.0	Jan 2018	Changes added as per CR1002	TSG	Jerome Hamel / 7Layers
4.1	June 2018	Updated with changes in CR1003	TSG	Jerome Hamel / 7Layers
5.0	July 2022	Updated with changes in CR1004	TSG#48 ISAG#21	Paul Gosden GSMA
6.0	May 2023	Updated with changes in CR1010	TSG#51 ISAG#30	Paul Gosden GSMA
7.0	Oct 2023	Updated with changes in CR1016	TSG#53 ISAG#34	Paul Gosden GSMA

D.2 Other Information

Type	Description
Document Owner	GSMA TSG
Editor / Company	Nicolas Damour Sierra Wireless

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.