# IoT DEVICE CERTIFICATION LANDSCAPE

SEPTEMBER 2019

# CONTENTS

# 1. Scope

This document walks the reader through the different types of certification used for an IoT Device, including regulatory approvals, telecoms industry certification and operator-specific tests. The main focus is on the telecoms industry certification from a 3GPP cellular connectivity perspective, where an overview of the certification process of GCF and PTCRB is provided. The document also explains where IoT Devices fit into certification processes originally intended for mobile phones and smartphones. References are made to existing test documentation and test plans where available.

# 2. Audience

This document is targeted at IoT Device manufacturers and users who need to understand the telecoms certification landscape in the regions where their devices will be deployed.

# 3. Introduction

Testing and certification programmes for cellular functionality has long been used as the means to ensure the correct functionality of mobile devices, such as smart phones and data dongles, when connecting to a cellular network. Fast forward to the world of the Internet of Things (IoT), where cellular connectivity is embedded into devices that historically had no associated connectivity, such as bicycles and water meters, and where the traditional testing and certification requirements could affect the adoption of such solutions.

Integrating cellular Communication Modules into devices that are not considered “typical” mobile devices, such as smart meters and location tracking devices, may trigger requirements for specific tests and certifications. These requirements may place a significant time and cost burden on vertical market IoT Device manufacturers to the extent that it becomes a barrier to entry for such devices across vertical market segments.

This document intends to provide information on the testing and certification options for IoT Devices with fully integrated cellular radio capabilities from a cellular functionality perspective. This document also provides a high level description of other types of certifications that may be required, for example, due to government regulations.

# 4. Why Certify a Cellular Device?

In the development and production of consumer smartphones, for example, manufacturers invest a huge amount of time and effort to ensure their smartphones conform to the 3GPP specifications and that they work correctly. Manufacturers would typically source Communication Modules or Radio Baseband Chipsets that have been certified and proven to work, and would ensure their smartphones are similarly certified. Smartphone manufacturers also have global scale enabling them to field trial their devices on many network configurations. The same resource and expertise for building smartphones may not be available for the development of IoT Devices. This is due to the limited resources available to IoT Device manufacturers, which may well mean that they do not have the resources to certify their devices, especially in the LPWA (low power wide area) market which is price-sensitive. As a result, there may be unforeseen issues which are uncovered when uncertified IoT Devices connect with the network.

Wherever network operators have a requirement for a cellular device to be certified, be it a smartphone or a cellular-based location tracker, the reasons are twofold. Certification ensures that devices do not have an adverse effect on the network or on other wireless devices in the vicinity. The other reason is to ensure interoperability, so that devices work as intended when connected to the operator's network. If devices do not work correctly on the network, a lot of time may be spent by the network operator and their customers to try to address the connectivity problem. Within an IoT project, such issues mean more project time is spent on the functionality of the cellular connectivity component, rather than focussing on the IoT application interaction.

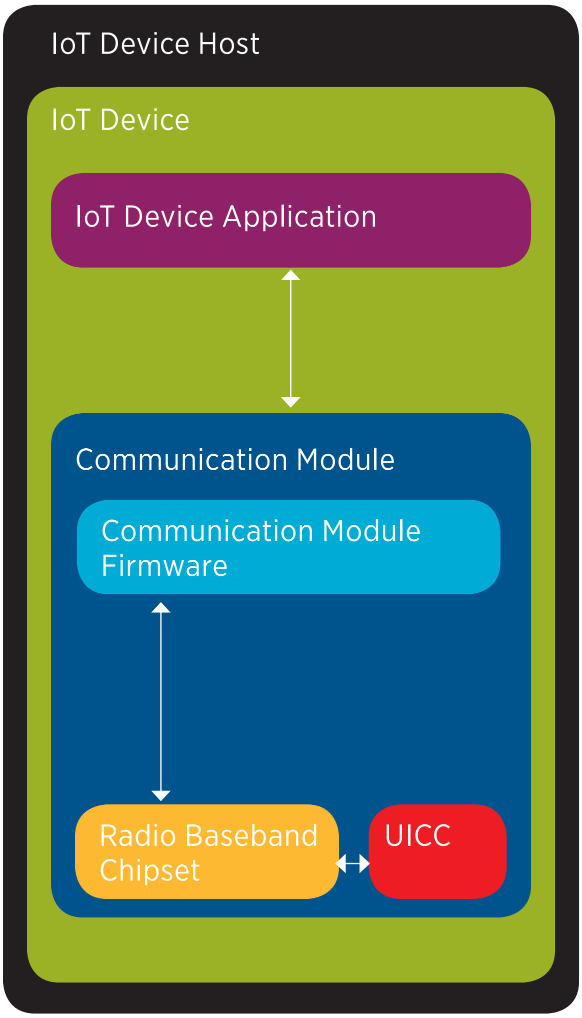
There are network operators that sell white-labelled devices, including IoT Devices, under the operator's brand. To ensure the devices work as intended and to minimise the impact on customer support teams, network operators perform rigorous testing of these devices before taking them to the market. These tests can be in addition to telecoms certifications such as GCF and PTCRB.

In the case where the network operator supplies SIM cards to an IoT service provider, there will often be a commercial requirement that the Communications Module has telecoms certification, along with the completion of additional operator-specific tests.

Cellular networks are typically configured differently from one region to the next, due to different market conditions and local requirements. So there are operators that require additional operator testing to ensure that devices work correctly with their specific network configuration. Furthermore, newer technologies such as LTE-M, NB-IoT and 5G enable high-performance use cases on both extremes of deployment scenarios.
In order to leverage these features properly, devices may need to be customised for the specific network configurations.

# 5. Definition of IoT Device

In order to have a clear understanding of the scope of the certification required, it is important to have a good view of the components that make up an IoT Device. The following diagram, adapted from GSMA TS.34[1], illustrates the different elements of an IoT Device and the terminology used throughout this document.



**IoT DEVICE HOST –** The application specific environment containing the IoT Device e.g. connected car, smart meter, security alarm etc.

**IoT DEVICE –** The combination of both the IoT Device Application and the Communication Module e.g. vehicle telematics unit.

**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.

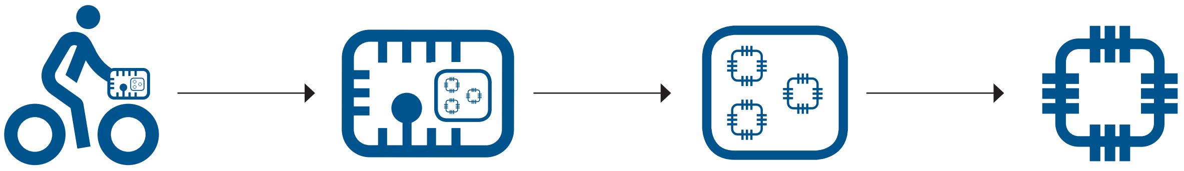
**COMMUNICATION MODULE –** The communications component which provides wide area (2G, 3G, 4G) radio connectivity. Comprising of Communications Module Firmware, Radio Baseband Chipset and UICC.

**COMMUNICATIONS MODULE FIRMWARE –** The functionality within the Communications Module that provides an API to the IoT Device Application and controls the Radio Baseband Chipset.

**RADIO BASEBAND CHIPSET –** The functionality within the communications module that provides connectivity to the mobile network.

**UICC –** The smart card used by a mobile network to authenticate devices for connection to the mobile network and access to network services.

This can be further illustrated by the following example of a connected bicycle:



IoT DEVICE HOST

- ➔ Connected Bicycle

IoT DEVICE

- ➔ Bicycle Application + Communications Module

COMMUNICATIONS MODULE

- ➔ Firmware + Baseband Radio Chipset + SIM card

RADIO BASEBAND CHIPSET

# 6. Overview of Certification Types

Certification requirements for devices used for IoT fall into three distinct categories, illustrated with examples, as follows:

REGULATORY CERTIFICATION / COMPLIANCE

TELECOM INDUSTRY CERTIFICATION

OPERATOR CERTIFICATION

## REGULATORY CERTIFICATION / TYPE APPROVAL

- These certifications are typically mandatory in order for electronics product to be sold in a specific market.
- The certifications are applicable to the IoT Device Host and / or IoT Device.
- The certifications usually demonstrate compliance with national regulations that cover, for example, safety aspects, and to ensure device RF emissions do not interfere with other wireless equipment. Examples include RF transmitter and receiver tests, electromagnetic compatibility (EMC), electrical safety and environmental.
- Depending on the intended use of the device, multiple regulatory agency approvals may be required.
- Examples include
  - China Compulsory Certification (CCC)
  - Electromagnetic Compatibility (EMC) Directive 2014/30/EU and Radio Equipment Directive (RED) 2014/53/EU
  - Federal Communications Commission (FCC) Part 18
  - Gijyutsu Kijyun Tekigō Shōmei (Giteki)
  - Network Access License (NAL)
- Depending on the market(s) where the device is intended to be sold or used, multiple regulatory certifications may be required with each market having its own regulatory body and approval process.

## INDUSTRY CERTIFICATION SCHEMES

- These certifications are typically in addition to the regulatory certification / type approval mentioned previously.
- These certifications check the functionality of the product, and whether the functionality conforms to specific industry standards by agreed conformance test suites, which may include interoperability testing and field testing.

## INDUSTRY CERTIFICATION SCHEMES: TELECOMS

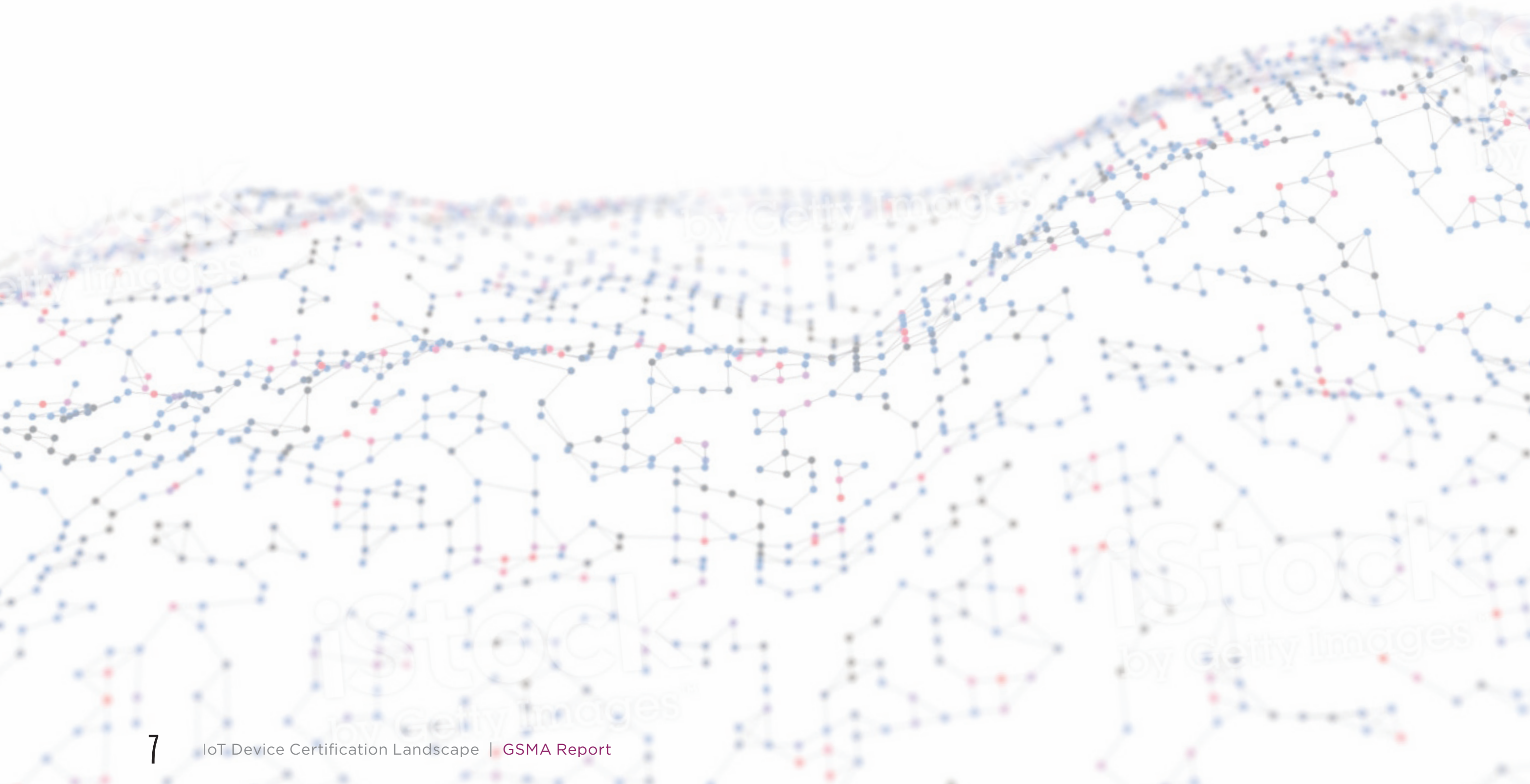
- The two main Telecoms Industry certification schemes are GCF and PTCRB which have different origins, which is reflected in differences in the way the schemes operate and their scope.
- GCF is a voluntary scheme that uses self-declaration with a quality assurance and certification challenge process. PTCRB is mandatory for devices that will use the networks of operators that are members of the scheme. Each PTCRB certification is verified with tests executed at PTCRB approved labs.
- Geographical scope of the schemes differ, with GCF used worldwide, including by some North American operators, and PTCRB used mainly in North America.
- Both schemes cover testing based on 3GPP standards, SIM/eSIM functionality and antenna performance. PTCRB adds North American specific requirements.
- As well as certification of mobile devices, both schemes also cover certification of IoT Devices and related components, such as Communication Modules. GCF also includes certification of service layer functionality such as oneM2M in partnership with the TTA.
- Both GCF and PTCRB do not currently have a distinct process for IoT Device certification, as both organisations use the same scheme as for mobile devices. However, as IoT devices are typically less complex than mobile devices, the testing involved is significantly less than a smartphone in order to achieve certification.
- The schemes also allow for Communication Module certification which can be integrated into an IoT Device enabling the re-use of test results.
- Network operators will often require one of the certification schemes to be obtained as part of their acceptance or certification requirements.

## INDUSTRY CERTIFICATION SCHEMES: VERTICAL INDUSTRY CERTIFICATION (FOR EXAMPLE AUTOMOTIVE, MEDICAL)

- These schemes may cover additional requirements on top of any regulatory certification and telecoms certification.
- They are related to end user safety and / or vertical-specific needs and environments, such as extreme operating temperatures and vibrations that are found inside vehicles.
- Automotive certification examples include IATF 16949 and ISO 9001 applicable to the production facilities, AEC-Q100, AED-Q200, ISO 26262 applicable to the IoT Device and IoT Device Host.

## OPERATOR-SPECIFIC CERTIFICATION

- Typically this is in addition to the Telecom Industry certification, where network operators execute additional interoperability testing specific to their network configuration and network parameter settings.
- Some operators may require industry certification, whereas others may treat such approvals as optional. In some cases, where the network operator accepts the results of Telecom Industry certification, additional operator-specific tests may not be required.
- Often, this testing focuses on in-field performance of the devices, such as radio sensitivity, dropped connection rate, handover success, data throughput and battery life.
- This certification is applicable for IoT Device Hosts, IoT Devices and Communication Modules and Radio Baseband Chipsets, covering IoT security, Service Layer and Application Layer, depending on the network operator requirements.
- Operator-specific certification may be required in order for the device to be used on a specific network or across a group of network operators, or in order to be sold via the network operator channels as either manufacturer-branded or white-labelled devices.
- For devices that will be roaming onto multiple networks, operator certification is typically only needed on the home network, i.e. the network that provides the cellular subscription.
- Examples of operator certification processes are described below:
    - AT&T: https://iotdevices.att.com/networkready.aspx
    - Deutsche Telekom: refer to Annex
    - Verizon: https://opendevelopment.verizonwireless.com/get-certified



# 7. Telecom Industry Certification for IoT

The organisations that are involved in the IoT certification process are:

- Global Certification Forum (GCF)
- PTCRB

## 7.1 GLOBAL CERTIFICATION FORUM (GCF)

GCF is an independent organisation that defines the certification framework for devices that are based on cellular technologies such as GSM, UMTS, LTE, NB-IoT and 5G from 3GPP. GCF operates based on vendor and operator membership, and has a number of working groups that take test specifications developed by organisations such as 3GPP and GSMA, and develop the certification criteria and test methods in order for vendor's devices to qualify for GCF certification. GCF certification is widely used in many regions and can be considered as a global certification body.

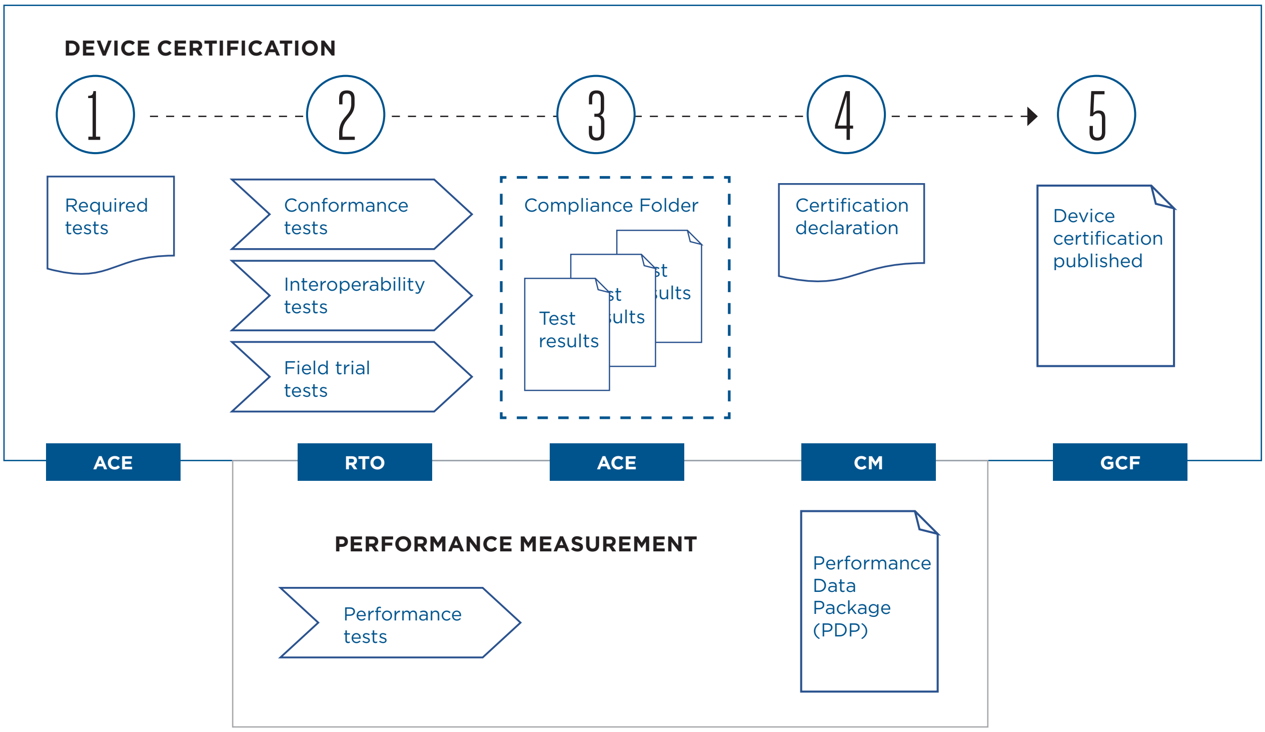
### 7.1.1 GCF CERTIFICATION PROCESS FOR IOT DEVICES

The first step before GCF certification can be obtained is GCF membership, as only GCF members may have their products certified.

Device manufacturers applying for GCF membership must also make a self-declaration that they have a recognised quality assurance programme in place for their design, development and manufacturing processes. In addition, manufacturers are required to indicate that they possess, or have subcontracted for, the skills and means of test to perform the self-assessment of their new product's conformity with the relevant GCF certification criteria. This involves the use of either an internal or third party Assessment Capable Entity (ACE) to determine the specific scope of testing, and the use of a GCF Recognised Test Organisation (RTO) to execute the testing.

The membership type depends on the manufacturer's in-house capabilities as well as the manufacturer product categories, and will dictate how much of the GCF certification process can be done in-house by the manufacturer, or whether an external organisation needs to be used.

A high level diagram showing the GCF device certification process is shown in the following diagram.



*Source:* GCF, 2019

**STEP 1:** The certification process starts with the definition of the scope of the tests for the certification. The manufacturer completes a “Declaration Summary” form indicating the technology supported by the device, such as the technology type, radio bands and other specific 3GPP features.

**STEP 2:** This form is reviewed by an Assessment Capability Entity (ACE), which is carried out by a GCF member with this capability[1], in order to determine the applicable test cases.

An IoT Device may qualify for an optimised GCF certification process[2] on the following conditions:

I. The embedded Communications Module is GCF-certified

II. The Communications Module GCF certification granted less than three years before the start of certification of the IoT Device in which it is embedded

III. The IoT Device primary functionality must be something other than to provide mobile communications, i.e. the IoT Device cannot be, for example, a smartphone

Note that a GCF certified Communications Module can be used for three years until it needs either to be recertified against the latest GCF-CC (Certification Criteria) version or replaced by a newly certified Communications Module.

[1] https://www.globalcertificationforum.org/certification/certification-process/ace/tpace.html
[2] https://www.globalcertificationforum.org/certification/certified-modules.html

The required set of tests for the optimised process also depend on:

I. The features and functions available on the IoT Device as declared by the manufacturer

II. Comparison of the features and functions available on the IoT Device compared with the GCF-certified

III. Whether the functionality of the Communications Module is affected by integration into the IoT Device

The test details for the optimised certification process are defined in GCF-CC [5] Annex G and associated Annexes F.x, which include:

- OTA antenna performance
- Power supply
- SIM interface
- Radiated emissions
- User interface
- Application enablers
- Audio (if applicable)

These tests focus on functions that are provided specifically by the IoT Device rather than the Communications Module.

**Step 3:** The tests are then executed by a GCF member designated as Recognised Test Organisations (RTO)[3] based on the GCF Certification Criteria. These include:

- Conformance tests
- Interoperability tests
- Field testing in commercial live network(s)
- And optionally, performance tests

**STEP 4:** The Assessment Capability Entity (ACE) reviews all the test results to verify if the device meets the relevant certification criteria.

**STEP 5:** Once a new product has successfully met all the relevant certification criteria, the manufacturer can declare it as having achieved the certified status and can submit the declaration to GCF. The appropriate documents to complete the registration are captured in the GCF Certification Criteria (GCF-CC) Permanent Reference Document.

### OTHER ITEMS TO NOTE

The manufacturer is also required to maintain appropriate traceable documentation to support this declaration in a 'Compliance Folder'. This documentation is kept up-dated for every device update and can be inspected by operators under bilateral conditions.

GCF-CC are continually updated with new or modified test cases and a product must be certified within the period for which a specific CC version is valid. Typically, a network operator will request certification to the latest GCF-CC. Timing is vital, especially when considering the schedule for integrating an already GCF certified Communications Module into an IoT Device and the start of actual testing with a network operator.

When a product is approved to a particular version, changes made to that product can also be approved to the original version, unless new features are added then the product must be approved to the current version.

More information of the GCF certification process can be found here[4] and here[5].

[3] https://www.globalcertificationforum.org/certification/certification-process/rto.html
[4] https://www.globalcertificationforum.org/certification/certification-process.html
[5] https://www.globalcertificationforum.org/certification/5-steps.html

### 7.1.2 LIST OF GCF CERTIFIED PRODUCTS

A list of GCF certified devices can be found here:
https://www.globalcertificationforum.org/products/all-certified-products.html

From a Mobile IoT perspective, the GCF has certification processes in place for LTE-M and NB-IoT technologies, and a number of modules with these technologies have been certified[6].

## 7.2 PTCRB (PCS TYPE CERTIFICATION REVIEW BOARD)

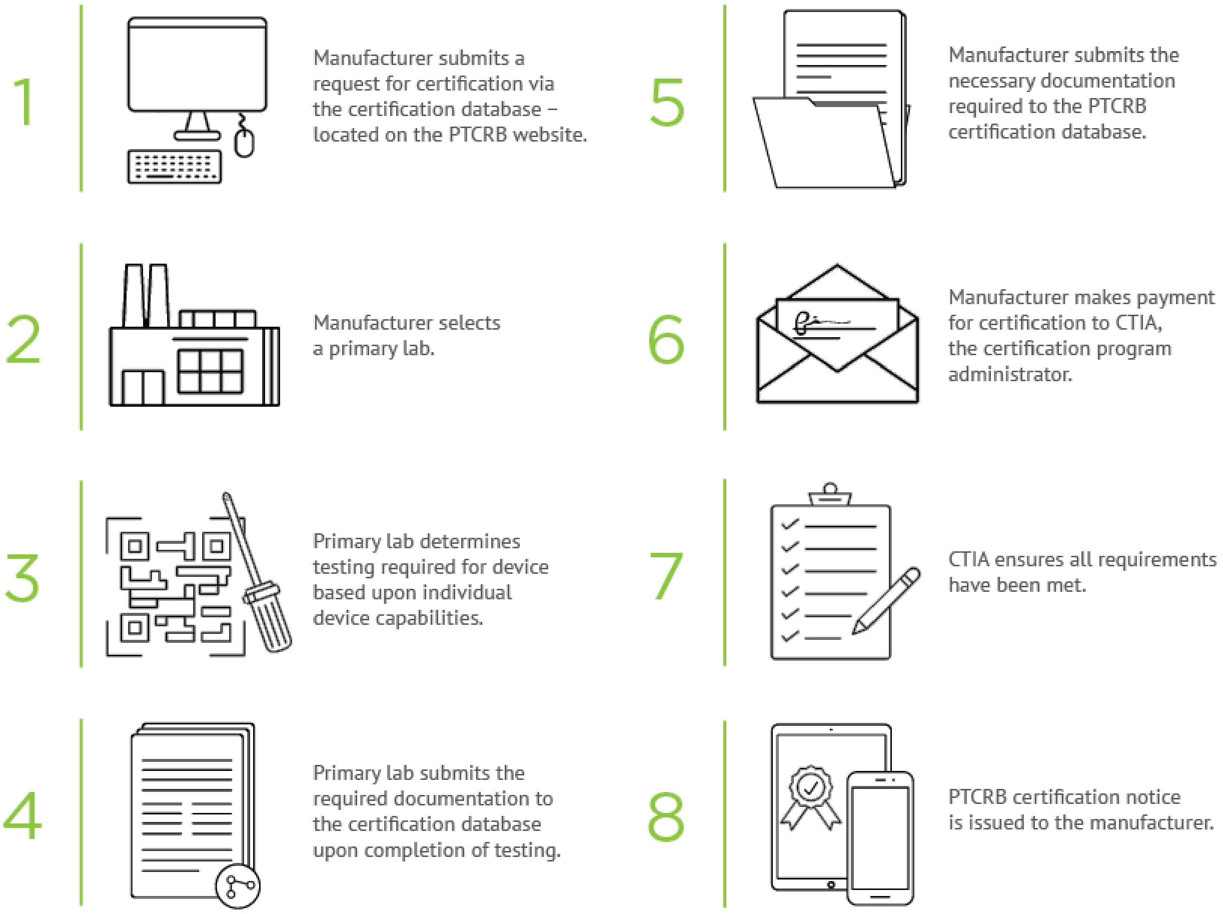
North American network operators established PTCRB as an independent organisation to provide the framework for cellular mobile devices and Communication Modules to obtain certification for use on PTCRB operator networks. PTCRB certification is considered regional, covering mainly North America.

The PTCRB membership includes network operators, device manufacturers and test labs. A PTCRB working group of authorised test labs own the test cases for PTCRB certification, which are based on the cellular technology specification such as 3GPP's UMTS and LTE. The administrator for the PTCRB certification process is CTIA.

[6] https://www.globalcertificationforum.org/iot-devices.html

### 7.2.1 PTCRB CERTIFICATION PROCESS FOR IOT DEVICES

The general PTCRB certification process is shown in the following diagram[7], which highlights the necessary steps a device manufacturer needs to take in order to obtain PTCRB certification. Note that PTCRB certification involves lab-based testing and not field testing.



1 Manufacturer submits a request for certification via the certification database – located on the PTCRB website.

2 Manufacturer selects a primary lab.

3 Primary lab determines testing required for device based upon individual device capabilities.

4 Primary lab submits the required documentation to the certification database upon completion of testing.

5 Manufacturer submits the necessary documentation required to the PTCRB certification database.

6 Manufacturer makes payment for certification to CTIA, the certification program administrator.

7 CTIA ensures all requirements have been met.

8 PTCRB certification notice is issued to the manufacturer.

*Source: PTCRB, 2019*

Where the device manufacturer embeds a PTCRB-certified Communications Module into the IoT Device, the number of tests that need to be done in order to achieve PTCRB certification is typically reduced to cover the device interfaces such as the SIM card, power and antenna.

A step-by-step guide for the IoT Device manufacturer to initiate the certification process, where a PTCRBcertified Communications Module is embedded in the device, is described here: https://www.ptcrb.com/wp-content/uploads/2018/12/How_to_Certify_an_Integrated_Device_R1-1.pdf

### 7.2.2 LIST OF PTCRB CERTIFIED PRODUCTS

A list of PTCRB certified devices can be found here: https://www.ptcrb.com/certified-devices/

[7] https://www.ptcrb.com/certification-program/

# 8. Certification Approach

IoT Device manufacturers understandably want to find the best and fastest route to market, while navigating the complexities of the certification needs of the various markets.

The manufacturers can follow the approach below to optimise their telecoms certification process:

PRODUCT DESIGN

- Determine target markets
- Comply with GSMA TS.34

PRODUCT DEVELOPMENT

- Use certified development and prototyping kits
- Use certified embedded Communications Modules and / or certified Chipset

TESTING

- Consult with mobile network operators

- Determine target market(s) in terms of region(s), country(ies) and network operator(s). This will help dictate the regulatory certification required, and whether GCF or PTCRB certification is needed
- Document best-practice design or product compliance to GSMA TS.34 [1][2]
- Consider using development and prototyping kits that have been certified
- Where possible, use off-the-shelf components to build the IoT Device:
  - Ensure the IoT Device uses a Communications Module already certified according to the requirements of the target markets(s) and / or mobile network operator(s). This may help reduce the tests needed to gain certification and minimise the cost of returns due to technical issues.
  - If the embedded Communications Module is not certified, consider whether the Chipset within the selected Communications Module has been certified: this can potentially expedite the certification process
- Consult with the mobile network operator to understand their certification requirements (if any); operators may have contractual conditions and / or tariffs that restrict usage of non-certified products on their networks
- Consult with mobile network operators, as they may have identified work-arounds for technical issues, which would be invaluable to consider for their implementation

# 9. Next Steps

One key requirement for operators is for IoT Devices to have a reasonable behaviour when these devices are using the mobile operator's network. To help ensure that IoT Device manufacturers have a clear understanding of the behaviour required, GSMA guidelines should be produced that include a set of self-assessment tests that manufacturers can perform and record their IoT Device's results. The tests should be based on the GSMA Connection Efficiency specifications [1][2].

## Definitions

| TERM | DESCRIPTION |
|---|---|
| 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 B aseband Chipset. |
| 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. |
| 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. |
| Mobile IoT | Mobile IoT is a GSMA term which refers to the 3GPP standardised Low Power Wide Area (LPWA) technologies using licensed spectrum bands such as LTE-M and NB-IoT. |
| Radio Baseband Chipset | The functionality within the Communications Module that provides connectivity to the mobile network. |
| UICC | The smart card used by a mobile network to authenticate devices for connection to the mobile network and access to network services. |

# Abbreviations

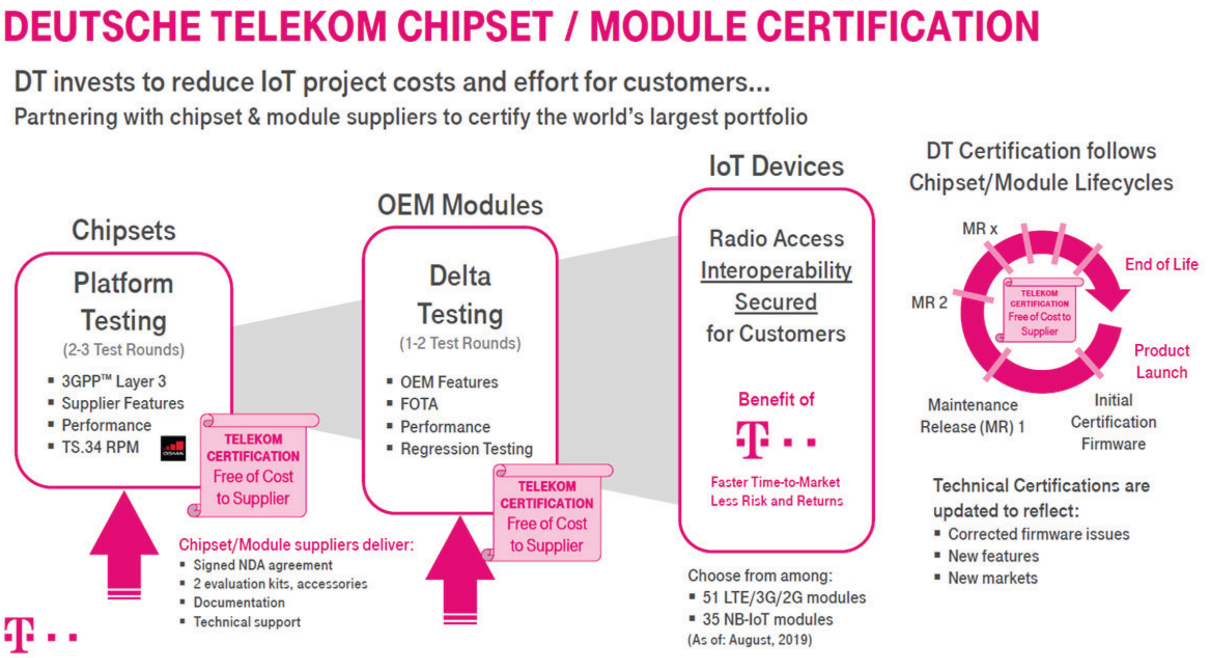
| TERM | DESCRIPTION |
|---|---|
| GCF | Global Certification Forum |
| IoT | Internet of Things |
| LTE-M | Long Term Evolution for Machine Type Communications |
| LPWA | Low Power Wide Area |
| M2M | Machine to Machine |
| NB-IoT | Narrow Band IoT |
| PTCRB | PSC Type Certification Review Board |
| UICC | Universal Integrated Circuit Card |

# References

| REF | DOCUMENT NUMBER | TITLE |
|---|---|---|
| [1] | GSMA TS.34 | IoT Device Connection Efficiency Guidelines<br>https://www.gsma.com/newsroom/resources/ts-34-iot-deviceconnection-efficiency-guidelines-version/ |
| [2] | GSMA TS.35 | IoT Device Connection Efficiency Test Book<br>https://www.gsma.com/newsroom/resources/ts-35-iot-deviceconnection-efficiency-test-book-version/ |
| [3] | GSMA TS.39 | Mobile IoT Test Requirements<br>https://www.gsma.com/newsroom/resources/ts-39/ |
| [4] | GSMA TS.40 | Mobile IoT Field and Lab Test Cases<br>https://www.gsma.com/newsroom/resources/ts-40-miot-fieldlab-test-cases/ |
| [5] | GCF CC | GCF Certification Criteria<br>https://www.globalcertificationforum.org/certification.html |

# ANNEX

One key requirement for operators is for IoT Devices to have a reasonable behaviour when these devices are using the mobile operator's network. To help ensure that IoT Device manufacturers have a clear understanding of the behaviour required, GSMA guidelines should be produced that include a set of selfassessment tests that manufacturers can perform and record their IoT Device's results. The tests should be based on the GSMA Connection Efficiency specifications [1][2].



## DEUTSCHE TELEKOM CHIPSET / MODULE CERTIFICATION

**DT invests to reduce IoT project costs and effort for customers...**

**Partnering with chipset & module suppliers to certify the world's largest portfolio**

Chipsets

Platform Testing

(2-3 Test Rounds)

- 3GPP™ Layer 3
- Supplier Features
- Performance
- TS.34 RPM

TELEKOM CERTIFICATION Free of Cost to Supplier

Chipset/Module suppliers deliver:

- Signed NDA agreement
- 2 evaluation kits, accessories
- Documentation
- Technical support

OEM Modules

Delta Testing

(1-2 Test Rounds)

- OEM Features
- FOTA
- Performance
- Regression Testing

TELEKOM CERTIFICATION Free of Cost to Supplier

IoT Devices

Radio Access Interoperability Secured for Customers

Benefit of T · ·

Faster Time-to-Market

Less Risk and Returns

Choose from among:

- 51 LTE/3G/2G modules
- 35 NB-IoT modules

(As of: August, 2019)

DT Certification follows Chipset/Module Lifecycles

MR x
End of Life
MR 2
TELEKOM CERTIFICATION Free of Cost to Supplier
Product Launch
Maintenance Release (MR) 1
Initial Certification Firmware

Technical Certifications are updated to reflect:

- Corrected firmware issues
- New features
- New markets

*Source:* *Deutsche Telekom, 2019*

For more information please visit:
www.gsma.com/IoT

**GSMA HEAD OFFICE**
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601