Project: H2020-ICT-688712

Project Name:

5G Applications and Devices Benchmarking (TRIANGLE)

Deliverable D2.2

Formalization of the certification process, requirements and use

Date of delivery:	30/06/2017	Version:	1.0
Start date of Project:	01/01/2016	Duration:	18 months

Deliverable D2.2

Formalization of the certification process, requirements and use

Project Number:	ICT-688712
Project Name:	5G Applications and Devices Benchmarking
Project Acronym	TRIANGLE

Document Number:	ICT-688712-TRIANGLE/D2.2
Document Title:	Formalization of the certification process, requirements and use
Lead beneficiary:	DEKRA Testing and Certification, S.A.U.
Editor(s):	DEKRA Testing and Certification, S.A.U.
Authors:	Keysight Technologies Belgium (Michael Dieudonne), Keysight Technologies Denmark (Andrea Cattoni, German Corrales Madueño), Universidad of Malaga (Alberto Salmerón, Almudena Díaz, Pedro Merino), Redzinc Services Limited (Donal Morris), DEKRA (O. Castañeda, C. Cardenas, J. Mora, J. Baños)
Dissemination Level:	PU
Contractual Date of Delivery:	30/06/2017
Work Package Leader:	DEKRA Testing and Certification, S.A.U.
Status:	Final
Version:	1.0
File Name:	TRIANGLE_D2-2.docx

Abstract

This document reviews existing certification schemes (both regulatory and private certifications) for LTE and Wi-Fi devices and applications and proposes a suitable certification scheme for pre 5G devices and applications according to the testing defined in this project.

Keywords

certification scheme, LTE, 5G, Wi-Fi

Executive summary

The main objective of this document is to define a certification scheme for TRIANGLE project. To achieve this objective, firstly, the mobile world existing certification schemes are reviewed, focusing on the specific requisites and certification process of each scheme. Based on this study and specific TRIANGLE requirements, TRIANGLE certification program is defined. Finally, the document defines the certification requirements that will be required for products obtaining TRIANGLE mark.

The document is divided in three parts.

Part 1 of this document reviews and analyzes the existing certification schemes for cellular and Wi-Fi technologies. Certification schemes can be divided into two major groups: Regulatory certifications and private certifications schemes.

Regulatory certifications, also known as type approval schemes, are certifications requested by an authority. These certifications are used to demonstrate compliance with some requirements established in national regulations.

The certification process, and the standards on which the certification process is based, are used by manufacturers to demonstrate that products comply with the relevant national legislation. At the level of the European Union, the process of demonstrating compliance with Directives is based on the use of harmonized standards.

A harmonised standard is a European standard developed by a recognised European Standards Organisation: CEN, CENELEC, or ETSI. It is created following a request from the European Commission to one of these organisations. Manufacturers, other economic operators, or conformity assessment bodies can use harmonised standards to demonstrate that products, services, or processes comply with relevant EU legislation.

In general, compliance with those requirements provides certain warranty of quality, interoperability, safety, immunity and/or efficiency in the use of some limited resources. This certification is mandatory to sell a product in a country or market.

However as regulatory certification is usually focused on essential requirements they do not warranty full interoperability with all network implementations. To avoid this problem, many industry organisations and telecom carriers have defined private certification programs.

There are two main groups defining private certification schemes: Industry certifications provided by Industry Alliances such as GCF, PTCRB or Wi-Fi and Carrier Certifications (also known as device acceptance programs) such those of Telefónica, AT&T certifications, T-Mobile, etc.

Part 2 of this document includes a proposal for TRIANGLE certification scheme. The proposal presented has been developed considering formal conformance testing methodology, based on ISO 9646 and other ETSI testing methodology approached derived from the ISO standard, the use of third party testing, based on the principles defined in ISO 17025, and an approach that can be easily adapted for use or recognition by well known and established industry alliances such as GCF.

Part 3 of this document defines TRIANGLE Test Specifications, their organization and contents as well as the process to write them.

Together with this document, several appendices are delivered which correspond to the TRIANGLE Test Specifications and other documents, such as TRIANGLE scoring, related to TRIANGLE certification process as detailed in Annex F of this document.

Contents

List of Figures

List of Tables

List of Appendices

Appendix	Title	Description
1	Scoring	Evaluation of products (device or app) performed according to the measurements and KPIs obtained during the testing.
2	Product characterization (ICS/IXIT)	ICS and IXIT tables used to define the main functionalities supported by the product and other additional functionality required to perform the certification testing
3	Test case Reference List (TCRL)	The TCRL includes the list of test cases included in the TRIANGLE Certification Program and the requirement to execute or not each single test case for a specific TRIANGLE Certification Program release.
4	Applications User Experience Test Specification	User Experience Test Specification for Apps.
5	Applications Resource usage Test Specification	Usage of device resources Test Specification for Apps.
6	Devices User Experience with reference Apps Test Specification	User Experience Test Specification for devices when using reference Apps
7	Applications Energy Consumption Test Specification	Energy consumption Test Specification for Apps.
8	Network scenarios parameterization	Defines the radio parameters to be used based on the TRIANGLE scenarios
9	IoT devices Energy Consumption Test Specification	User Experience Test Specification for IoT devices (Emergency services).
10	IoT devices Data Performance Test Specification	Data Performance for IoT devices (Emergency services).
11	IoT devices Reliance Test Specification	Data Performance for IoT devices (Emergency services).

List of Abbreviations

3GPP	3rd Generation Partnership Project
ACE	Assessment Capable Entity
AGPS	Assisted GPS
AP	Access Point
API	*Application Programming Interface*
BSMI	Bureau of Standards, Metrology and Inspection
CAPI	Control API
CC	Certification Criteria
CCC	China Compulsory Certification
CE	Conformité Européenne
CSFB	Circuit Switched Fallback
CTIA	Cellular Telephone Industries Association
CTT	Certification Test Tool
CWG-RF	Converged Wireless Group RF Performance
DCC	Devices Certification Criteria
DoC	Declaration of Conformity
DUT	Device Under Test
EAP	Extensible Authentication Protocol
EPC	Evolved Packet Core
EU	European Union
E-UTRA	Evolved Universal Terrestrial Radio Access
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
FRN	FCC Registration Number
GCF	Global Certification Forum
GPO	Government Printing Office
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile communications
HCI	Host Controller Interface

Hz	Hertz
IBSS	Independent Basic Service Set
ICS	Implementation Conformance Statement
IoT	Internet of Things
ISC	Internet Systems Consortium
IXIT	Implementation eXtra Information for Testing
KCC	Korea Communications Commission
M2M	Machine to Machine
MNO	Mobile Network Operator
NB	Notified Body
LATAM	LATin AMerica
LSF	Lighting Service Framework
LTE	Long Term Evolution
OEM	Original equipment manufacturer
OTA	Over The Air
PC	Personal computer
PTCRB	PCS Type Certification Review Board
QoS	Quality of Service
RF	Radio Frequency
RTO	GCF Recognised Test Organisation
UMA	Universidad de Málaga
UTRA	Universal Terrestrial Radio Access
SAR	Specific Absorption Rate
SIM	Subscriber Identity Module
STA	Station
SWP	Single Wire Protocol
TCB	Telecommunication Certification Body
TDD	Time Division Duplex
TDLS	Tunnelled Direct Link Setup
TIS	Total Isotropic Sensitivity
TRP	Total Radiated Power

TTS	Telefónica Test Specification
UCC	Unified CAPI Console
UICC	Universal Integrated Circuit Card
USAT	*USIM* Application Toolkit
USIM	Universal Subscriber Identity Module
UE	User Equipment
UMA	Universidad de Málaga
USB	Universal Serial Bus
VCCI	Voluntary Council for Control of Interference
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access

1 Existing Certification Schemes

There are two major types of certification schemes in the certification market: Regulatory Certifications (also named type approval) and private certification schemes.

Regulatory are mandatory certification schemes required by Authorities to be able to sell a product in a specific country or market. Examples are the CE marking in European countries and FCC in the USA.

Private certification schemes can be also be divided into two major groups: Industry Certifications such as GCF or PTCRB, and Carrier Certifications.

Industry certification schemes are usually associated with the right to use an Industry Alliance protected logo. The right to use the logo is as a result of the grant of the certificate and provides wide visibility to final users. Inside industry certification schemes we can also differentiate between cellular technologies and other technologies used by the mobile phones.

Carrier Certifications are usually device acceptance schemes from specific Mobile Network Operators such as Telefónica or AT&T. They are typically used when a vendor wants to use the operator as a commercial channel. I.e., the device, and in some cases the App, is commercialized under the name of the operator.

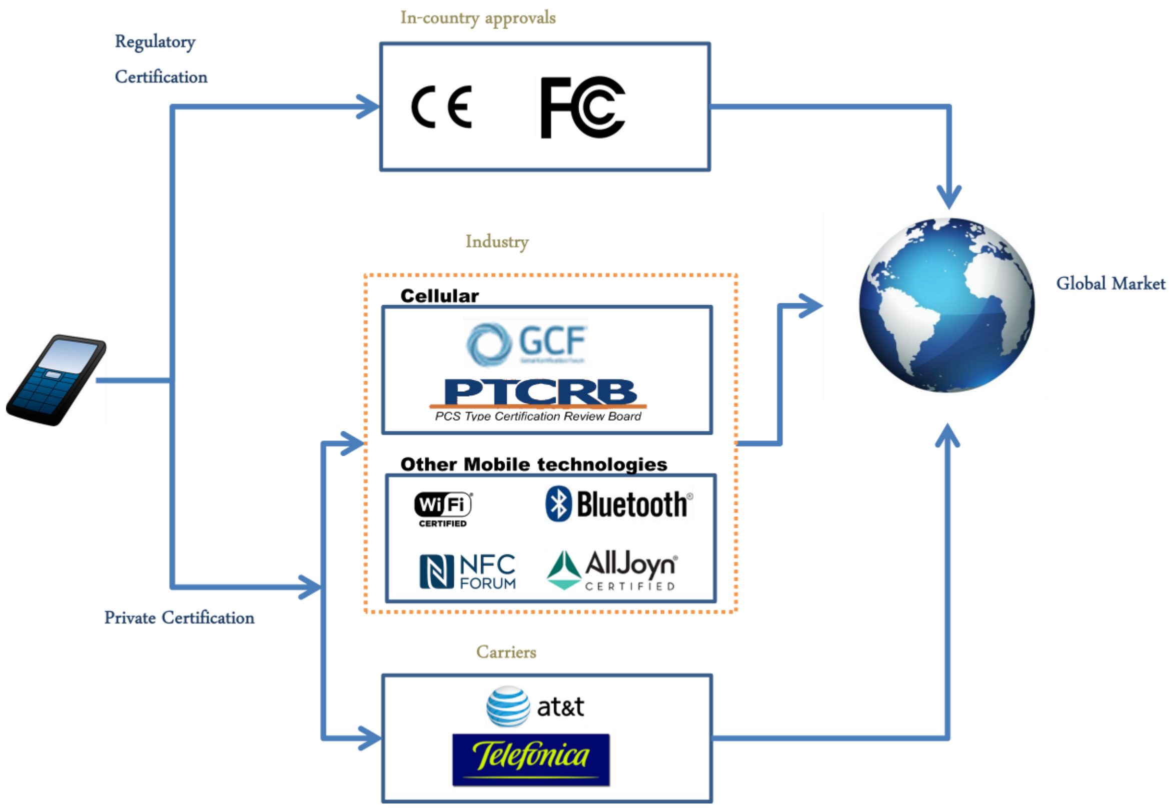


Figure 1 – Certification process

A vendor needs to consider a number of factors before defining the certification strategy for a product and the scope of testing to undergo. The geographic area and the carriers to sell a device are key decisions to make early in the development process, as these decisions affect important product decision choices, including frequency bands, features, user interface, etc.

After basic product business decisions are taken and the device is finally designed and developed, but before the product can be punt in the market, the required certifications must be obtained.

Normally, testing required for regulatory certifications is the first testing to be performed. Failing regulatory testing will mostly imply basic hardware changes in the design of the product, and these changes will thus affect other testing performed so far.

CE marking and/or FCC testing is usually the first regulatory testing to be performed. Passing this testing normally means that the product will pass regulatory testing in other countries or regions the product market is targeted to.

After regulatory certification is granted, the next logical step for cellular devices, is usually is to undergo GCF and/or PTCRB industry certifications as these certifications are normally an entry requirement for most network operators. Neither GCF nor PCTRB certification is mandatory, but GCF certification is usually recognized by European network operators, while PTCRB certification is recognized by many US network operators.

GCF and PTCRB are certification schemes that incorporate testing for configurations and features agreed among the carriers that are members of the alliances. However before granting access to the commercial channel, carriers want to ensure the device, and sometimes the Apps, fully interwork with the particular configuration or configuration of their own network and their services. To guarantee certain level of interworking and performance most of the larger carriers have defined their own device acceptance schemes (carrier certification schemes).

Even if a device is already GCF and/or PTCRB-certified most of the larger operators will require the device to undergo a device acceptance program (carrier certification scheme) to enter the carrier distribution channel. Carriers with device acceptance certification schemes (also referred as “homologation” or “qualification” by some carriers) include AT&T, Verizon, T-Mobile, the main carriers in the USA; Telefónica, one of the main operators in Europe, etc.

Figure 2 lists examples of the main existing certification schemes, both regulatory certification and private (industry and carriers) certifications.

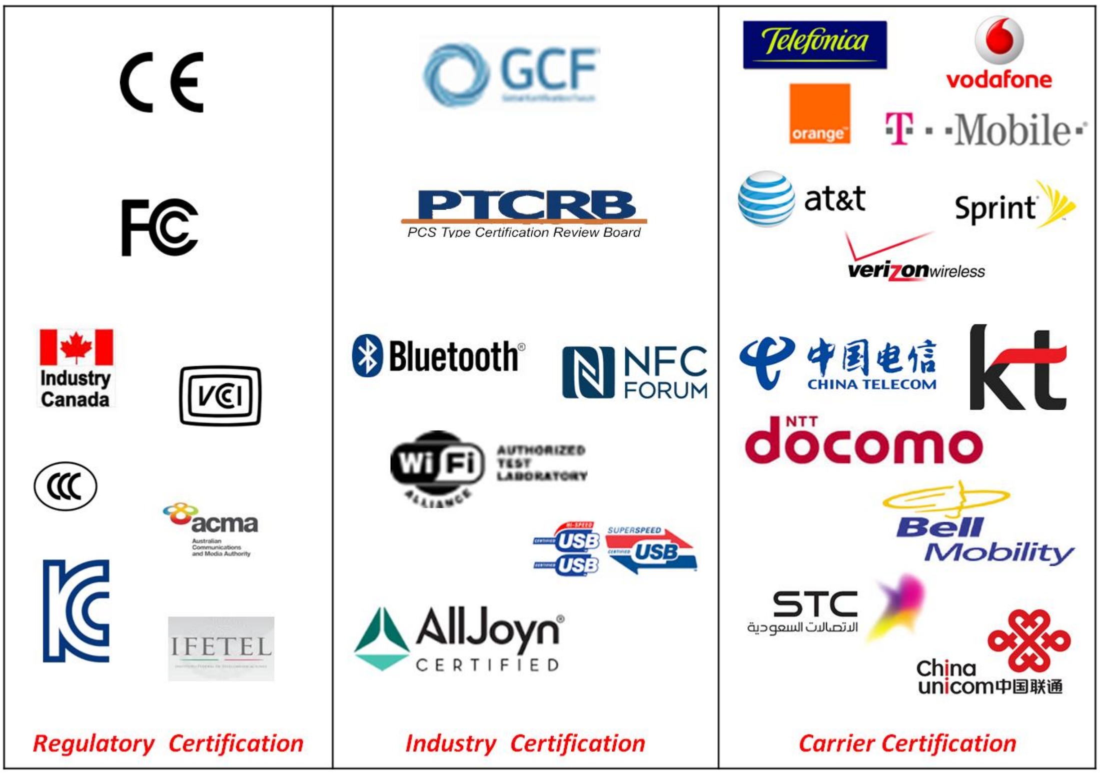


Figure 2 – Representative Certification Schemes

Note: All trademarks and trade names are of their respective owners.

Cellular phones, or in general any UE device, may also support other technologies. Relevant examples of other typical technologies supported by smartphones include Wi-Fi, Bluetooth, ZigBee, etc.

To comply with the license agreement (as it is the case for Bluetooth) or to get the right to use the widely recognized by final users logo mark (as it is the case for Wi-Fi) the product has to undergo Industry Alliances Certification Schemes. Each industry consortium or alliance certification requirements and priorities is different, however most of them focus on ensuring interoperability through testing conformance to the industry standard or test plan and interoperability in pre-define testbed configurations.

1.1 Regulatory Certification Schemes

Relevant government authorities define certain mandatory requirements to allow the commercialization of products in a specific country or region.

Regulatory Certification Schemes are needed to demonstrate compliance with some requirements established by the national (or regional) regulation. The compliance with those requirements provides certain warranty of quality, interoperability, safety, immunity and/or efficiency in the use of some limited resources

They are also legally required to import/commercialise or/and use a product.

Most relevant regulatory certifications are FCC (USA) and CE marking (European Union) as they involve large markets that are also reference for other regions (see figure 2 for some examples).

1.1.1 General Aspects

The authority defines a specific procedure to demonstrate the compliance with some requirements:

- Technical requirements.
  - Radio, EMC, Electrical safety, Health/SAR, Telecom.
- Legal requirements: As part of the approval procedure it is needed to comply with some legal requirements to get the approval (e.g. dealer's license of the approval holder).
- Post-approval requirements.
  - Labeling.
  - Packaging.
  - User manual.

1.1.1.1 Regulatory aspects to take into account for LTE devices

There are a few aspects that need to be specially taken into account when looking for regulatory certification of an LTE device in different countries and markets. The most relevant are:

- Frequency allocation.
- Antenna gain.

Frequency Allocation

Radio spectrum is a very limited resource, and is managed independently by each country's regulatory authority. In order to allocate spectrum to a mobile operator, the national regulatory authority has to make sure that spectrum is not being used by any other services (radar, military communications, etc.).

As a result of this, the allocation of spectrum for mobile services is rather country-dependent.

The spectrum allocated for LTE varies around the world and as a result there many LTE bands and frequency allocations.

FDD spectrum requires pair bands, one for the uplink and one for the downlink, and TDD requires a single band as uplink and downlink are on the same frequency but on different time slots.

There are very many frequency bands used for LTE TDD and FDD versions. Table 1 summarizes existing LTE bands (3GPP TS 36.101 v14.3.0 (2017-03)).

Even if an LTE device supports several bands, the regulator will define which bands are allowed to be used in its specific country.

Table 1 - Table example: Items

E-UTRA Operating Band	Uplink (UL) operating band BS receive UE transmit	Downlink (DL) operating band BS transmit UE receive	Duplex Mode
	F_{UL_low} – F_{UL_high}	F_{DL_low} – F_{DL_high}	
1	1920 MHz – 1980 MHz	2110 MHz – 2170 MHz	FDD
2	1850 MHz – 1910 MHz	1930 MHz – 1990 MHz	FDD
3	1710 MHz – 1785 MHz	1805 MHz – 1880 MHz	FDD
4	1710 MHz – 1755 MHz	2110 MHz – 2155 MHz	FDD
5	824 MHz – 849 MHz	869 MHz – 894MHz	FDD
6[1]	830 MHz – 840 MHz	875 MHz – 885 MHz	FDD
7	2500 MHz – 2570 MHz	2620 MHz – 2690 MHz	FDD
8	880 MHz – 915 MHz	925 MHz – 960 MHz	FDD
9	1749.9 MHz – 1784.9 MHz	1844.9 MHz – 1879.9 MHz	FDD
10	1710 MHz – 1770 MHz	2110 MHz – 2170 MHz	FDD
11	1427.9 MHz – 1447.9 MHz	1475.9 MHz – 1495.9 MHz	FDD
12	699 MHz – 716 MHz	729 MHz – 746 MHz	FDD
13	777 MHz – 787 MHz	746 MHz – 756 MHz	FDD
14	788 MHz – 798 MHz	758 MHz – 768 MHz	FDD
15	Reserved	Reserved	FDD
16	Reserved	Reserved	FDD
17	704 MHz – 716 MHz	734 MHz – 746 MHz	FDD
18	815 MHz – 830 MHz	860 MHz – 875 MHz	FDD
19	830 MHz – 845 MHz	875 MHz – 890 MHz	FDD
20	832 MHz – 862 MHz	791 MHz – 821 MHz	FDD
21	1447.9 MHz – 1462.9 MHz	1495.9 MHz – 1510.9 MHz	FDD
22	3410 MHz – 3490 MHz	3510 MHz – 3590 MHz	FDD
23	2000 MHz – 2020 MHz	2180 MHz – 2200 MHz	FDD
24	1626.5 MHz – 1660.5 MHz	1525 MHz – 1559 MHz	FDD
25	1850 MHz – 1915 MHz	1930 MHz – 1995 MHz	FDD
26	814 MHz – 849 MHz	859 MHz – 894 MHz	FDD
27	807 MHz – 824 MHz	852 MHz – 869 MHz	FDD
28	703 MHz – 748 MHz	758 MHz – 803 MHz	FDD
29	N/A	717 MHz – 728 MHz	FDD[2]
30	2305 MHz – 2315 MHz	2350 MHz – 2360 MHz	FDD
31	452.5 MHz – 457.5 MHz	462.5 MHz – 467.5 MHz	FDD
32	N/A	1452 MHz – 1496 MHz	FDD[2]
33	1900 MHz – 1920 MHz	1900 MHz – 1920 MHz	TDD
34	2010 MHz – 2025 MHz	2010 MHz – 2025 MHz	TDD
35	1850 MHz – 1910 MHz	1850 MHz – 1910 MHz	TDD

36	1930 MHz – 1990 MHz	1930 MHz – 1990 MHz	TDD
37	1910 MHz – 1930 MHz	1910 MHz – 1930 MHz	TDD
38	2570 MHz – 2620 MHz	2570 MHz – 2620 MHz	TDD
39	1880 MHz – 1920 MHz	1880 MHz – 1920 MHz	TDD
40	2300 MHz – 2400 MHz	2300 MHz – 2400 MHz	TDD
41	2496 MHz 2690 MHz	2496 MHz 2690 MHz	TDD
42	3400 MHz – 3600 MHz	3400 MHz – 3600 MHz	TDD
43	3600 MHz – 3800 MHz	3600 MHz – 3800 MHz	TDD
44	703 MHz – 803 MHz	703 MHz – 803 MHz	TDD
45	1447 MHz – 1467 MHz	1447 MHz – 1467 MHz	TDD
46	5150 MHz – 5925 MHz	5150 MHz – 5925 MHz	TDD[8,9]
…			
64	Reserved	Reserved	
65	1920 MHz – 2010 MHz	2110 MHz – 2200 MHz	FDD
66	1710 MHz – 1780 MHz	2110 MHz – 2200 MHz	FDD[4]
67	N/A	738 MHz – 758 MHz	FDD[2]

NOTE 1: Band 6 is not applicable

NOTE 2: Restricted to E-UTRA operation when carrier aggregation is configured. The downlink operating band is paired with the uplink operating band (external) of the carrier aggregation configuration that is supporting the configured Pcell.

NOTE 3: A UE that complies with the E-UTRA Band 65 minimum requirements in this specification shall also comply with the E-UTRA Band 1 minimum requirements.

NOTE 4: The range 2180-2200 MHz of the DL operating band is restricted to E-UTRA operation when carrier aggregation is configured.

NOTE 5: A UE that supports E-UTRA Band 66 shall receive in the entire DL operating band

NOTE 6: A UE that supports E-UTRA Band 66 and CA operation in any CA band shall also comply with the minimum requirements specified for the DL CA configurations CA_66B, CA_66C and CA_66A-66A.

NOTE 7: A UE that complies with the E-UTRA Band 66 minimum requirements in this specification shall also comply with the E-UTRA Band 4 minimum requirements.

NOTE 8: This band is an unlicensed band restricted to licensed-assisted operation using Frame Structure Type 3

NOTE 9: In this version of the specification, restricted to E-UTRA DL operation when carrier aggregation is configured.

LTE frequency of operation goes up to 6 GHz. 5G frequency of operation goes up to 52 GHz as defined for NR (New Radio) Phase 1.

Table 2 lists defined frequency ranges and supporting companies.

Table 2 – New frequency ranges for NR Release 15

Frequency Range	Supporting companies
3.3 - 4.2 GHz	NTT DOCOMO, CMCC, KDDI, SBM, China Telecom, Orange, etc.
4.4 - 4.99 GHz	NTT DOCOMO, CMCC KDDI, SBM, China Unicom, China Telecom, etc.
24.25 - 29.5 GHz	NTT DOCOMO, CMCC, KT, Verizon, T-mobile, Telecom Italia, etc.
31.8 - 33.4 GHz	Orange, Telecom Italia and British Telecom
37 - 40 GHz	AT&T, Verizon and T-mobile

Antenna gain

In some countries, such as Japan, there is a limitation on the maximum antenna gain so this parameter must be taken into account when developing an LTE device (for detailed information also check the Ordinance Regulating Radio Equipment (Radio Regulatory Commission Rules No. 18 of 1950) Notification.

Additionally, the antenna gain can influence the compliance to other requirements (e.g., spurious emissions), so these considerations should be taken in the early stage of the development.

1.1.2 European Union (CE marking)

In general, any product must be CE marked before it can be put in the EEA (EU + Iceland, Lichtenstein and Norway) market. There are a number of directives covering the requirements for CE marking. CE marking proves that a product had been assessed and meets EU safety, health and environmental protection requirements. The requirements and “certification” process is described in European directives which make reference to harmonized standards. These harmonized standards are published in the European Journal. Certification is valid for products manufactured both inside and outside the EEA, that are marketed inside the EEA.

CE marked products sold in the EEA have been assessed to meet high safety, health, and environmental protection requirements.

To affix the CE marking to a product, a technical dossier proving that the product fulfils all the EU-wide requirements must be put together. The product's manufacturer bears sole responsibility for declaring conformity with all requirements. Once the product bears the CE marking, the product's manufacturer might have to provide its distributors and/or importers with all the supporting documentation concerning CE marking.

The EU-wide requirements are laid down in directives that cover different products or product sectors.

1.1.2.1 Telecom equipment Certification requirements

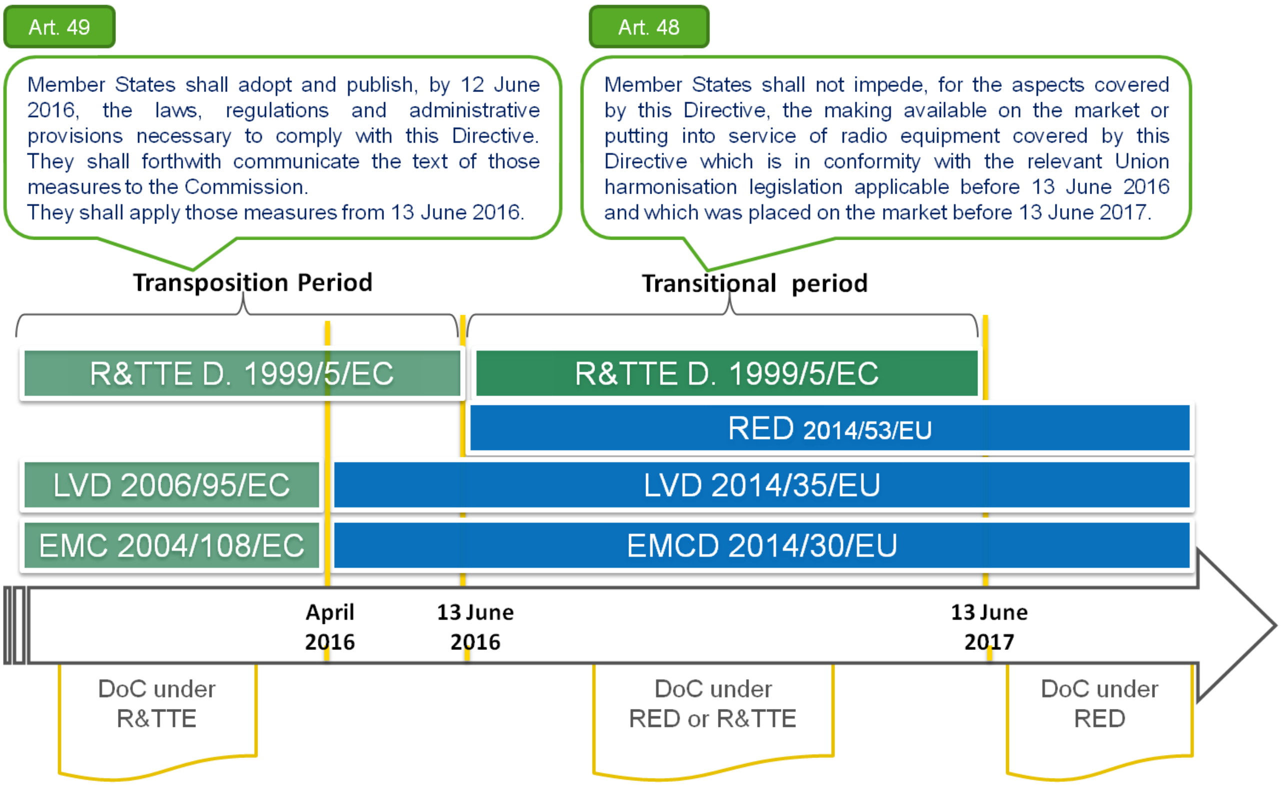
The Radio and Telecommunication Terminal Equipment Directive 1999/5/EC establishes a regulatory framework for placing and putting into service radio and telecommunications terminal equipment (R&TTE) on the free market. The European Parliament and Council

Directive on Radio and Telecommunication Terminal Equipment (1999/5/EC) was revised in 2014 to become the Radio Equipment Directive 2014/53/EU (RED).

This new directive is applicable as of June 13th 2016 and aligns the previous directive with the New Legislative Framework for the marketing of products.

The revision has taken into account the need for improved market surveillance, in particular for the traceability obligations of manufacturers, importers and distributors. It provides improved instruments for market surveillance, such as the possibility to require prior registration of radio equipment, within those categories affected by low levels of compliance.

Figure 3 shows the transitional period between the use of Directive 1999/5/EC and RED Directive 2014/53/EU.


Art. 49

Member States shall adopt and publish, by 12 June 2016, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith communicate the text of those measures to the Commission.
They shall apply those measures from 13 June 2016.

Art. 48

Member States shall not impede, for the aspects covered by this Directive, the making available on the market or putting into service of radio equipment covered by this Directive which is in conformity with the relevant Union harmonisation legislation applicable before 13 June 2016 and which was placed on the market before 13 June 2017.

Figure 3 – R&TTE to RED Timeline - Transition Dates

The RED Directive ensures a single market for radio equipment by setting essential requirements for safety and health, electromagnetic compatibility and the efficient use of the radio spectrum.

RED Directive covers equipment using the radio frequency spectrum, (i.e., which intentionally transmits or receives radio waves for communications or radiodetermination and Operating below 3.000 GHz (no lowest frequency limit)).

The general principles for product compliance in the RED Directive are:

- Compliance with essential requirements.
- Harmonised Standards provide a presumption of conformity with essential requirements.
- Conformity assessment procedures.

- Use of a Notified Body where no radio Harmonised Standard exists.

1.1.2.2 Steps to obtain CE marking

These are a number of steps that manufacturers need to follow to obtain CE marking:

1. Identify the EU requirements for the product to obtain the CE marking.

The EU-wide requirements are laid down in directives that cover different products or product sectors. Additional information can be found at https://ec.europa.eu/growth/single-market/european-standards_en.

2. Check whether the product meets the specific requirements.

It is up to the manufacturer to make sure its product meets all the EU legal requirements. If harmonised European standards exist for the product and the manufacturer follows them in the production process, the product will be presumed to be in conformity with the requirements laid down in the relevant EU directives. Harmonised European standards may be accessed at http://ec.europa.eu/growth/single-market/european-standards/harmonised-standards.

The use of standards is voluntary. The manufacturer is not obliged to use them. It can also opt for other technical solutions to fulfil the essential requirements set out in the relevant EU directive.

3. Check whether the product must be assessed by a Notified Body.

For some products, special conformity assessment bodies ('Notified Bodies') must verify that the product meets the specific technical requirements. This is not obligatory for all products.

4. Test the product.

If the product does not need to be verified by an independent body, then it is up to the manufacturer to check that it conforms to the technical requirements. This includes estimating and documenting the possible risks when using the product.

5. Compile the technical dossier.

The technical dossier should include all the documents that prove that the product conforms to the technical requirements.

6. Affix the CE marking and draft a declaration of conformity.

Finally the manufacturer can affix the CE marking on the product. The marking must be visible, legible and indelible. If a notified body was involved in step 3, the identification number of this body should also be put on the product. An EU declaration of conformity must also be drafted and signed stating that the product meets all legal requirements.

As from 12 June 2018, manufacturers shall register radio equipment (within some categories) within a central system (made available by the commission) prior to place that radio equipment on the market.

1.1.2.3 Harmonised standards

A harmonised standard is a European standard developed by a recognised European Standards Organisation: CEN, CENELEC, or ETSI. It is created following a request from the European Commission to one of these organisations.

The following table summarizes the conformance requirements and R&TTE related harmonised standards to be used to verify the fulfilment of those requirements for telecom devices using 2G&3G&LTE and Wi-Fi technologies.

Table 3 – R&TTE Harmonised standards

Requirement	**Technology**	**Harmonised standard**	**Description**
Safety (R&TTE, Article 3.1a)	All	EN 60950-1:2006 + A11:2009 + A12:2011 + A1:2010 + AC:2011 + A2:2013	Information technology equipment - Safety - Part 1: General requirements
Health (R&TTE, Article 3.1a)	All	EN 50360:2001 + AC:2006 + A1:2012	Product standard to demonstrate the compliance of mobile phones with the basic restrictions related to human exposure to electromagnetic fields (300 MHz - 3 GHz)
		EN 62311:2008	Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz - 300 GHz)
EMC (R&TTE, Article 3.1b)	All	EN 301 489-1 v12.1.1	Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
	2G	EN 301 489-7 v1.3.1	Part 7: Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS)
	3G & LTE	EN 301 489-24 v1.5.1	Part 24: Specific conditions for IMT-2000 CDMA Direct Spread (UTRA) for Mobile and portable (UE) radio and ancillary equipment
	Wi-Fi	EN 301 489-17 v2.2.1	Part 17: Specific conditions for Broadband Data Transmission Systems
Radio Spectrum (R&TTE, Article 3.2)	2G	EN 301 511 v9.0.2	Global System for Mobile communications (GSM); Harmonized EN for mobile stations in the GSM 900 and GSM 1800 bands.
	3G & LTE	EN 301 908-1 v7.1.1	IMT cellular networks;
	Wi-Fi 2.4GHz	ETSI EN 300 328 v1.9.1	Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques.
	Wi-Fi 5GHz	ETSI EN 301 893 v1.7.1	Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN

In the case of RED directive, no harmonised standard have been defined for Safety, health and EMC. Table 4 lists the conformance requirements defined by RED directive related to the Radio Spectrum and the corresponding harmonized standards

Table 4 – RED Harmonised standards

Requirement	Technology	Harmonised standard	Description
Radio Spectrum (RED, Article 3.2)	2G	EN 301 511 v9.0.2	Global System for Mobile communications (GSM); Harmonized EN for mobile stations in the GSM 900 and GSM 1800 bands. Note: This R&TTE harmonised standard provides presumption of conformity with the essential requirements of Directive 2014/53/EU if also the receiving parameters in clause(s) 4.2.20, 4.2.21 and 4.2.26 are applied.
	3G & LTE	EN 301 908-1 v11.1.1	Introduction and common requirements
	3G	EN 301 908-2 v11.1.1	IMT cellular networks
	LTE	EN 301 908-13 v11.1.1	Evolved Universal Terrestrial Radio Access (E-UTRA) User Equipment
	Wi-Fi 2.4GHz	ETSI EN 300 328 v2.1.1	Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques
	Wi-Fi 5GHz	ETSI EN 301 893 v2.1.1	5 GHz RLAN;

1.1.3 USA (FCC)

The Code of Federal Regulations, Telecommunications (title 47 of the United States Code of Federal Regulations) contains the U.S. federal regulations for telecommunications.

The official rules are published and maintained by the Government Printing Office (GPO) in the Federal Register.

The FCC regulates radio frequency (RF) devices contained in electronic-electrical products that are capable of emitting radio frequency energy by radiation, conduction, or other means. These products have the potential to cause interference to radio services operating in the radio frequency range of 9 kHz to 3000 GHz.

FCC does not specify the technology that equipment has to employ. If the equipment complies with the requirements established in the FCC rules, it will be certified regardless of the technology it uses.

As a general rule, products that, by design, contain circuitry operating in the radio frequency range need to demonstrate FCC compliance through one of the FCC's three different equipment authorization procedures depending on the type of device as specified in the FCC rules:

- Verification.
- Declaration of Conformity (DoC).
- Certification.

1.1.3.1 Equipment Authorization Procedures

There are three different approval procedures for equipment authorization. The specific procedure that is required to be used is based on the relative likelihood of causing harmful interference. The procedures are:

- **Certification** is an equipment authorization issued by the Commission or grant of Certification by a recognized TCB (Telecommunication Certification Body) based on an application and test data submitted by the responsible party (*e.g.,* the manufacturer or importer).

  The testing is done by a testing laboratory listed as approved by the Commission for performing such work.

  The Commission or a TCB examines the test procedures and data to determine whether the testing followed appropriate protocols and the data demonstrates technical and operational compliance with all pertinent rules.

  Technical parameters and other descriptive information for all certified equipment submitted in an application for Certification are published in a Commission-maintained public database, regardless of whether it is approved by the Commission or a TCB.

- **Declaration of Conformity (DoC)** is a procedure that requires the party responsible for compliance to use an accredited testing laboratory that follows established measurement protocols to ensure that the equipment complies with the appropriate technical standards.

  The responsible party must provide a test report and other information demonstrating compliance with the rules upon request by the Commission.

- **Verification** is a procedure that requires the party responsible for compliance to rely on measurements that it or another party makes on its behalf to ensure that the equipment complies with the appropriate technical standards.

1.1.3.2 Steps to get a product approved under FCC requirements

The following summary provides seven steps to help determine which approval procedure applies to a device (product) and the basic steps to getting that device approved under the FCC requirements:

1. Determine if device is a Radio Frequency (RF) device subject to the FCC rules.

   If a device is subject to FCC rules, determine the specific type of equipment authorization that applies to the device. Become familiar with all the basic marketing, equipment authorization, and importation rules. In some instances, a device may have different functions resulting in the device being subject to more than one type of approval procedure.

2. Determine all applicable technical and administrative rules that apply to the device requiring an equipment authorization.

   The technical requirements are generally specified in the applicable FCC rule parts and the administrative rules are specified in https://www.ecfr.gov/cgi-bin/text-idx?SID=559c2517d13bb8eb61784a74c01cb901&mc=true&node=pt47.1.2&rgn=div5%22%20\l%20%22sp47.1.2.j%22%20\o%20%2247%20CFR%20Part%202,%20Subpart.

3. Perform the required tests to ensure the device complies with the applicable technical requirements.

The type of testing facility (laboratory) used to demonstrate compliance is based on the required approval procedure.

- **Verification**: Equipment is required to be tested, but it is not required to use a FCC Recognized Testing Laboratory. The test laboratory used is required to maintain a record of the measurement facilities.
- **Declaration of Conformity**: Equipment is required to be tested by an FCC Recognized Accredited Testing Laboratory. The Commission maintains a list of the FCC Recognized Accredited Testing Laboratories.
- **Certification**: Equipment is required to be tested by an FCC Recognized Testing Laboratory. Prior to July 13, 2016, a Laboratory listed at FCC Section 2.948 can also perform the testing.

4. Once the testing is complete and the device is found to be in compliance, finalize the approval process based on the applicable approval procedure:
   - **Verification:**
     - The responsible party as specified in the rules warrants that each unit of equipment complies with the applicable FCC rules.
     - The responsible party maintains all of the required documentation demonstrating compliance with the applicable FCC rules.
   - **Declaration of Conformity**
     - The responsible party prepares a compliance information statement to be supplied with the product at the time of marketing.
     - The responsible party maintains all of the required documentation demonstrating compliance with the applicable FCC rules.
   - **Certification**
     - The responsible party, typically the manufacturer, obtains an FCC Registration Number (FRN) for a device requiring Certification. The FRN is a 10-digit number used to identify the individual or organization doing business with the FCC. The same FRN will be used for future approvals.
     - The responsible party obtains a Grantee Code from the Commission. A grantee code is required the first time a party applies for certification and can be used for all future approvals.
     - The responsible party applies to a Telecommunication Certification Body (TCB) for a grant of certification. An application for equipment authorization requires submission of information about the product. The applicant must submit the required information to a TCB for review as part of the certification process.
5. Label the product and provide the required customer information: Labeling Guidelines (KDB Publication 784748) provides detailed information about how to perform this procedure.
6. Maintain all documentation as part of the responsibility for retention of records and ensure that the manufactured products are in compliance.
7. Follow the import requirements and complete/file FCC Form 740 when importing products into the United States.

1.1.3.3 Certification of transmitter devices

Certification of transmitter devices is covered under FCC Rule Parts 11, 15, 18, 22, 24, 25, 27, 74, 80, 87, 90, 95, 97, and 101.

FCC set requirements for both intentional and unintentional radiation of transmitter devices.

Unintentional radiation

The Federal Communications Commission (FCC) requires most digital devices sold in the United States to meet the requirements of (CFR 47) rule part 15, subpart b.

The FCC rule part 15b focuses on “unintentional” radiation or noise generated by a digital device. This noise could potentially impact the operation of other devices in a close proximity and therefore requires testing of the unintentional radiators.

The FCC 15b is a self-declaration process, not a certification. There is no certificate or document received from the FCC once the testing is completed.

Intentional radiation

Additionally, the FCC has decided that all devices that are intentional radiators, in the FCC frequency spectrum, must receive an FCC certification.

Radio, wireless, transmitting equipment has to be tested by an FCC authorized testing lab in order to be in compliance with the FCC Rules / FCC Standards. Failure to comply can be serious including fines, product recalls, and prosecution by the FCC.

Table 5 indicates the requirements that need to be fulfilled by an LTE device that may include other technologies such as 2G, 3G, Bluetooth, Wi-Fi and/or NFC.

Table 5 – FCC Requirements for an LTE device

Requirement	**47 CFR Regulation**	**Section**	**Description**	**Band**
EMC	Part 15 Subpart B	15.107	Unintentional radiators. Conducted limits	150 kHz to 30 MHz
		15.109	Unintentional radiators. Radiated emission limits	30 MHz to above 960 MHz
Radio	Part 15 Subpart C	15.225	Intentional radiators. For NFC devices.	13.110–14.010 MHz
		15.247	Intentional radiators. Operations within the bands (for Wi-Fi devices and Bluetooth devices)	2400-2483.5 MHz & 5725-5850 MHz
	Part 15 Subpart E	15.407	Unlicensed National Information Infrastructure Devices: General technical requirements. For bands: For Wi-Fi devices	5150-5250 MHz, 5250-5350 MHz, 5470-5725 MHz & 5725-5850 MHz
	Part 22 Subpart H	22.913	Effective radiated power limits	869-894 paired with 824-849 MHz *GSM850; 3G & LTE band 5*
		22.917	Emission limitations	
	Part 24 Subpart E	24.232	Power and antenna height limits	1850-1910 MHz & 1930-1990 MHz *PCS1900; 3G &*
		24.238	Emission limitations for Broadband PCS	

Requirement	**47 CFR Regulation**	**Section**	**Description**	**Band**
			equipment	*LTE bands 2 and 25*
	Part 27	27.50 (a)	Technical requirements	2.3 GHz *LTE Band 30*
		27.53.(a).2	Emission limits	
		27.50 (h).2	Technical requirements	2.5 GHz *LTE bands 7 and 38*
		27.53.(m)	Emission limits	
		27.50 (b).9, 27.50 (b).10 & 27.50 (c).9	Technical requirements	698-806 MHz *LTE Bands 12, 13, 14 and 17*
		27.53.(c), 27.53.(d), 27.53(e), 27.53(f), 27.53(g)	Emission limits	
		Part 90 Subsection 90.531	758–775 MHz & 788–805 MHz public safety bands	
		27.50 (d).2	Technical requirements	1710–1755 & 2110–2155 MHz *3G & LTE Bands 4*
		27.53(l)	Emission limits	
Health/ SAR	Part 27 Section 27.52	1.1307	Actions that may have a significant environmental effect	-
		1.1310	RF radiation exposure limits	
		2.1091	RF radiation exposure evaluation: Mobile devices	
		2.1093	RF radiation exposure evaluation: Portable devices	
		KDB Publication 941225	SAR test procedures for devices incorporating Long Term Evolution (LTE) capabilities	
Electrical Safety	No requirements // UL mark or equivalent			

1.1.4 Other countries

Different countries have different regulations. Regulatory certifications of some relevant markets are:

China:

There are three main agencies taking care of different regulation aspects:

- Radio: The State Radio Monitoring Center (SRRC), http://www.srrc.org.cn/english, is a technical agency, under the Ministry of Industry and Information Technology, for the state radio regulation of China.
- EMC and Safety: The CCC (China Compulsory Certificate), http://www.cqc.com.cn/www/english/ProductCertification/CCC, is handled by the China Quality Certification Centre http://www.cqc.com.cn/www/english, a professional

certification body under China Certification & Inspection Group (CCIC) approved by State General Administration.

- Equipment connected to public network: The NAL (Network Access License): http://www.tenaa.com.cn/Default.aspx is a mandatory license for telecommunication equipment that is connected to the public telecommunication network. Vendors of radio equipment need to submit an application at the Ministry of Industry and Information Technology for receiving the NAL license.

Japan:

Radio equipment that can be connected to the telecom network needs to comply against:

- For Radio equipment: against the Radio Law
- For telecom equipment: against the Telecommunication Business Law.

Both laws are under the responsibility of the Minister of Internal Affairs and Telecommunications (MIC): http://www.tele.soumu.go.jp/e/index.htm.

Taiwan:

The equipment has to cover requirements set by two different authorities:

- The National Communications Commission (NCC), http://www.ncc.gov.tw/english/index.aspx# is the authority responsible for regulating telecommunications and broadcasting services. It established requirements for Radio equipment:
- The BSMI (Bureau of Standards, Metrology and Inspection) established EMC and safety requirements for telecommunication equipment.

Table 6 shows an overview of some other markets, just as a reference of country requirements across the world.

Table 6 – Other markets overview

	Kuwait	Kenya	Australia	Argentina	South Africa	Mexico
Local holder required	No	Yes	Yes	Yes	Yes	Yes
FCC or EU test reports and approval accepted (from accredited lab)	Yes	Yes	Yes	No	Yes	Yes
In-country testing required	No	No	No	Yes	No	No
Health requirements	No	Yes	Yes	No	No	No
Language	English	English	English	Spanish	English	Spanish
Approval Body	MoC	CA	ACMA	ENACOM	ICASA	IFETEL

1.2 Private Certification Schemes

Regulatory type approval is usually focused on some essential requirements and do not warranty correct interoperability or interface with the networks and all its features. To avoid this problem, many industry organisations have defined private certification programs.

Private certification schemes in the mobile industry may be divided into cellular schemes focused on cellular technologies (GSM, UMTS, LTE, etc.) and other certification schemes involving complementary technologies used by smartphones such as Wi-Fi or Bluetooth.

The two most important cellular certification schemes are those defined by GCF and PTCRB.

The main difference between both schemes is that GCF is conducted under a cooperative voluntary basis and PTCRB is driven by operators. GCF and PTCRB certifications are not mandatory, but GCF operators are free to purchase phones having or not GCF certification while PTCRB operators are not allowed to purchase non-PTCRB-certified phones.

Figure 4 shows the most recognized Testing & Certifications schemes that apply to a smartphone including cellular and additional technologies.

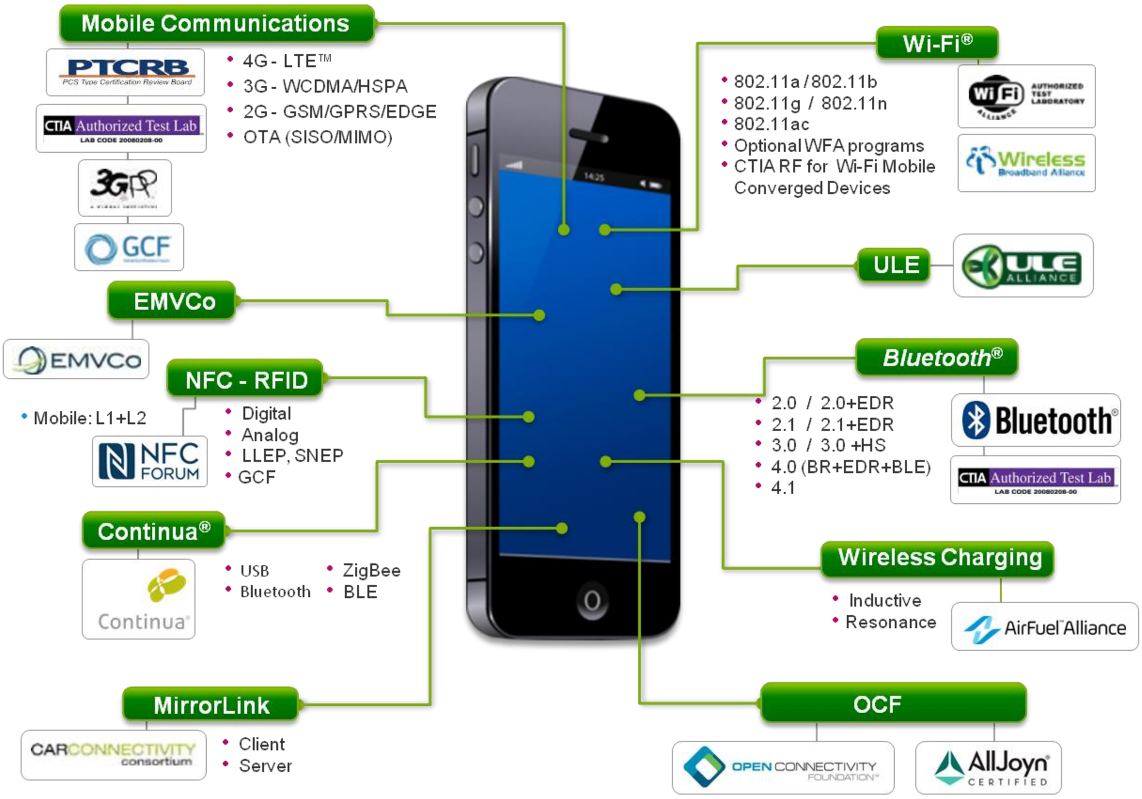


Figure 4 – Industry most relevant certification schemes for smartphones

1.2.1 Cellular Certification Schemes

There are two main cellular certification schemes: GCF and PTCRB. Smart phones manufactures will usually certify their products for both schemes. Although both schemes are not mandatory, most operators will require these certifications in order to sell the terminals, this way manufacturers are pushed to certify their products.

PTCRB is required for most North American operators and many South American operators mainly. GCF is required by operators in Europe and all around the world.

1.2.1.1 GCF

Certification Forum (GCF) is an active partnership between network operators, device manufacturers and the test industry.

GCF has created an independent certification programme to help ensure global interoperability between mobile devices and networks and to verify the compliance of wireless devices to agreed standards. GCF establishes global best practice for the certification of mobile phones and the range of devices that incorporate wireless connectivity.

The GCF scheme evolves according to developments in mobile technologies. GCF currently covers cellular technologies such as LTE. Wi-Fi technology is not included in GCF certification scheme, but it is part of the private Wi-Fi Alliance certification scheme.

GCF certification follows the principles of a Supplier's declaration of conformity (SDoC) [ISO/IEC 17050]: The responsibility for certification, and the maintenance of products certification, are fully accepted and assured by the certifying manufacturer. Evidence for the product conformance is detailed in a supporting Compliance Folder produced and maintained by the Certifying Organisation.

Certification Program

To become certified, a device needs to be assessed against all the Certification Criteria that have been defined for each technology and functionality incorporated within the device.

An Assessment Capable Entity (ACE) determines which tests are required for each new device. All testing must be undertaken by a GCF Recognised Test Organisation (RTO).

GCF requires that Conformance testing is performed in ISO 17025 accredited laboratories to ensure quality, impartiality and consistency.

The detailed requirements applicable for the purposes of Certification are defined in the GCF-CC document (GCF Certification Criteria) and the Devices Certification Criteria (DCC) database.

GCF-CC document (GCF Certification Criteria) references the core design requirements defined in technical specifications of a GCF recognized Standards Organisation and additional design specifications or recommendations which may be relevant for GCF.

GCF-CC requirements include, among others, LTE requirements according to standards:

- 3GPP TS 36.521-2 "User Equipment (UE) conformance specification; Radio transmission and reception; Part 2: Implementation Conformance Statement (ICS)".
- 3GPP TS 36.523-2 “User Equipment (UE) conformance specification; Part 2: Implementation conformance statement (ICS) specification” for E-UTRA devices

GCF-CC also specifies the Test Platforms to be used to execute every single test case. These Test Platforms need to have been previously validated.

GCF-CC is released four times per year according to the meeting schedule.

Test Specifications included in the GCF Certification program are listed in Table 7.

The manufacturer, normally supported by the main Test Lab selected for GCF certification, will determine the certification test plan applicable to the product under certification based on GCF-CC release selected.

1.2.1.2 PTCRB

PTCRB is a certification forum initially established by North American cellular operators.

PTCRB was created to establish a third party certification, giving confidence to the operator that the certified device meets a minimum set of requirements established by the members. This gives confidence to the operator that their roaming partner's device will not cause harm.

The PTCRB consists of representatives from all GERAN, UTRA and E-UTRA operators that declare membership, test labs (accredited by PTCRB), and the certification administrator (CTIA).

The purpose of the PTCRB is to provide the framework within which GERAN, UTRAN, and E-UTRAN device certification can take place for members of the PTCRB.

Certification Program

PTCRB certification is a voluntary process by which all products are technically evaluated to meet the minimum requirements for registration on the PTCRB Operators' networks.

Obtaining PTCRB Certification for a mobile device ensures compliance with 3GPP network standards within the PTCRB Operators' networks. Consequently, PTCRB Operators may block devices from their network if they are not PTCRB certified.

PTCRB certification is based on standards developed by 3GPP, OMA and other SDOs recognized by PTCRB. In some cases, PTCRB certification may accommodate North American standards and additional requirements from the FCC, Industry Canada, or any other government agency that may have jurisdiction and/or competence in the matter.

PTCRB operators may also develop and approve additions and/or modifications to the PTCRB requirements.

Additionally, PTCRB attempts to harmonize PTCRB certification with the GCF (Global Certification Forum) certification program.

This process is recommended for all manufacturers who wish to have their devices operating within the areas served by PTCRB Operators, as all PTCRB Operator full members require PTCRB Certification.

The certification process is supported at the PTCRB certification database accessible via www.ptcrb.com.

The manufacturer will submit a request for certification, selecting a primary lab. The primary lab will be responsible for all testing done on the device. The Test Lab will elaborate a Certification Test Plan, i.e., the list of all the testing required based on the devices capabilities.

The PTCRB permanent reference document, NAPRD.03 [10], contains the technical devices certification test and assessment requirements.

NAPRD03 is released four times per year according to the meeting schedule.

NAPRD03 advises accredited laboratories on how to establish terminal equipment conformity with the reference specifications. NAPRD03 clearly identifies the conformance requirements and the reference test systems configuration to be used to perform the evaluation, as defined on the PTCRB TC Database (test cases database).

The reference test systems need to be validated for each single test case by a PTCRB test lab before the may be used for products' certification.

PTCRB TC Database provides a separate listing of the test cases. Only PTCRB registered users may access TC database.

PTCRB Program Management Document (PPMD) [11] provides the framework within which GERAN, UTRA and E-UTRA device certification can take place.

PTCRB requires testing all bands supported by the device and inside PTCRB scope regardless of what bands its target carrier may use. As an example, T-Mobile uses slightly different bands than most North American GSM operators. So, a manufacturer intending to sell a product to T-Mobile operator will have to test on the 850 MHz band even though T-Mobile does not use that band.

GCF and PTCRB Reference Specifications

GCF and PTCRB reference specification list is detailed in Table 7.

Table 7 – GCF and PTCRB Test Specification list

Technology	Test Specification	Test Items	GCF	PTCRB
2G	*3GPP TS 51.010*	RF, Protocol and SIM	Yes	Yes
	3GPP TS 51.010-4	SIM Application Toolkit	Yes	Yes
3G	3GPP TS 34.121	Radio Frequency	Yes	Yes
	3GPP TS 34.123	Protocol	Yes	Yes
	3GPP TS 31.121	USIM	Yes	Yes
	3GPP TS 31.124	USAT	Yes	Yes
	3GPPTS 26.132	Audio	Yes	Yes
	ETSI TS 102 230	UICC; Physical, electrical and logical interfaces	Yes	Yes
	ETSI TS 102 384	UICC; Card Application Toolkit	Yes	Yes
	3GPP TS 34.124	Electromagnetic compatibility	No	Yes
	3GPP TS 34.171	A-GPS. FDD	Yes	Yes
	3GPP TS 37.571	UTRA, E-UTRA and EPC UE positioning	Yes	Yes
LTE	3GPP TS 36.121	Radio Frequency	Yes	Yes
	3GPP TS 36.123	Protocol	Yes	Yes

Technology	Test Specification	Test Items	GCF	PTCRB
	3GPP TS 36.124	Electromagnetic compatibility	Yes	Yes
UICC (NFC)	ETSI TS 102 694-1	SWP (Single Wire Protocol), a communication protocol between a mobile handset and a UICC that enables the NFC application to reside on the U-ICC).	Yes	Yes
	ETSI TS 102 695-1	HCI (Host Controller Interface), provides a logical interface on top of the SWP to support the creation of a host network and support contactless applications on the UICC	Yes	Yes
	GSMA TS.27	NFC Handset Test Book	Yes	No
Application Enablers (AEs) / Services	OMA-IOP-MMS-ETS (v1.1, v1.2 and v1.3)	Multimedia Messaging Service	Yes	Yes
	OMA-ETS-SUPL-v2.0 (and v1.0)	Secure User Plane Location	Yes	Yes
	OMA-ETS-DM v1.2	Device Management	Yes	Yes
	OMA-ETS_XHTMLMP_CON v1.2	Browsing. XHTML Mobile Profile	No	Yes
	OMA-ETS-WCSS-v1.1	Browsing. Wireless CCS	No	Yes
	OMA ETS FUMO v1.0	Firmware Update Management Object	No	Yes
	OMA ETS SCOMO v1.0	Software Component Management Object	No	Yes
	OMA-ETS-RCS-v5.1	Rich Communication Services	Yes	No
	IMTC 3G-324M	Video telephony	No	Yes
	3G-324M	Video Telephony Activity Group Conformance & IOP test cases	No	Yes
	3GPP TS 34.229-1	IMS	No	Yes
	PTCRB Bearer-Agnostic TTY Test Specification, v 1.0	TTY, (telecommunications feature for hearing and speech impaired people)	No	Yes
	2G TTY Test Specification, v 4.31	2G TTY	No	Yes
	TTY 3G Test Specification, v 2.0	3G TTY	No	Yes
	PTCRB PVG.03	PTCRB defined additional test cases	No	Yes
	PTCRB Bearer Agnostic AT-Command Test	AT commands	No	Yes

Technology	Test Specification	Test Items	GCF	PTCRB
	Specification			
Performance	CTIA OTA Test Plan	A-GPS Radiated performance	No	Yes
	CTIA/Wi-Fi Alliance Test Plan for RF Performance Evaluation of Wi-Fi Mobile Converged Devices	Mobile Station RF Performance Evaluation	No	Yes
	CTIA Test Plan for LTE Interoperability	Mobile Station RF Performance Evaluation	No	Yes (Optional)
	GCF-PC. PI-001	GCF Performance Criteria. Battery Life Measurement	Yes (Optional)	No
	GCF-PC. PI-002	Acoustic Performance Measurements	Yes (Optional)	No
	GCF-PC. PI-004	Antenna Performance – FS-Speech-Browsing mode	Yes (Optional)	No
	GCF-PC. PI-005	Data Throughput	Yes (Optional)	No
	GCF-PC. PI-0017	LTE –OTA Antenna Performance	Yes (Optional)	No

1.3 Other Industry Private Certification Schemes

1.3.1 Wi-Fi Alliance

Wi-Fi Alliance® is a non-profit organization that promotes Wi-Fi® technology and certifies Wi-Fi products if they conform to certain standards of interoperability.

The Wi-Fi Alliance owns the globally recognized Wi-Fi trademark "Wi-Fi CERTIFIED". Wi-Fi Alliance also owns the following brands: Wi-Fi®, Wi-Fi CERTIFIED™, Wi-Fi Protected Access®, Wi-Fi Multimedia™, Wi-Fi ZONE™, WMM®, WPA™, WPA2™, Wi-Fi Protected Setup™, Wi-Fi Direct®, Wi-Fi CERTIFIED Passpoint®, Passpoint®, Wi-Fi CERTIFIED Miracast™, Miracast®, Wi-Fi Aware™, Wi-Fi CERTIFIED HaLow™, Wi-Fi CERTIFIED WiGig™, Wi-Fi CERTIFIED Vantage™, Wi-Fi Vantage™, Wi-Fi CERTIFIED TimeSync™,Wi-Fi TimeSync™, Wi-Fi CERTIFIED Location™ and Wi-Fi CERTIFIED Home Design™.

Wi-Fi CERTIFIED products have undergone extensive testing by an independent Authorized Test Laboratory. When a product passes testing successfully, the manufacturer or vendor is granted the right to use the Wi-Fi CERTIFIED logo. Certification means that a product has been tested in numerous configurations with a diverse sampling of other devices to validate interoperability with other Wi-Fi CERTIFIED equipment operating in the same frequency band.

Wi-Fi CERTIFIED products will have greater chances to interoperate with other Wi-Fi products than otherwise and will deliver good user experience. Certification testing includes radio and data format interoperability, but also security protocols and optional testing for power management and quality of service protocols.

The objective of certification testing is to demonstrate that Wi-Fi CERTIFIED products will perform correctly in networks together with other Wi-Fi products.

Certification is available for a wide range of consumer, enterprise, and operator-specific products, including smartphones, appliances, computers and peripherals, networking infrastructure, and consumer electronics.

A company must be a member of the Wi-Fi Alliance to have its products tested for certification and to use the Wi-Fi CERTIFIED logo and associated trademarks.

Wi-Fi Alliance members have certified more than 25,000 products.

1.3.1.1 Certification Programs

Wi-Fi Alliance certification programs cover the following categories [1]:

- Connectivity.
- Security.
- Access.
- Applications and Services.
- Optimization.
- RF Coexistence

Wi-Fi Alliance certification programs are detailed below and classified according to the existing categories.

Connectivity

- Interoperable connectivity: 'Wi-Fi CERTIFIED a' in 5 GHz and 'Wi-Fi CERTIFIED b/g' in 2.4 GHz.
- Advanced Wi-Fi: 'Wi-Fi CERTIFIED n' in both 2.4 and 5 GHz for high-performance Wi-Fi networking.
- 'Wi-Fi CERTIFIED ac', the very latest version of Wi-Fi in 5 GHz, pushing Wi-Fi past the gigabit-per-second data rate milestone for network capacity.
- 'Wi-Fi Direct', allows Wi-Fi client devices that connect directly without use of an access point, to enable applications such as printing, content sharing, and display. Wi-Fi Direct certifies products which implement technology defined in the Wi-Fi Peer-to-Peer Technical Specification.

Security

- WPA2 (Wi-Fi Protected Access 2): Wi-Fi wireless network security offers government-grade security mechanisms for both personal and enterprise environments.
- EAP (Extensible Authentication Protocol): A set of authentication mechanisms used to validate the identity of network devices in the enterprise.
- Protected Management Frames: Wi-Fi CERTIFIED WPA2 with Protected Management Frames extends WPA2 protection to unicast and multicast management action frames, which is playing an increasing role in advanced Wi-Fi applications.

Access

- Passpoint: Enables SIM and non-SIM mobile devices to discover, select and connect to Wi-Fi networks without user intervention. Passpoint certifies products which implement technology defined in the Wi-Fi Alliance Hotspot 2.0 Technical Specification.
- Wi-Fi Protected Setup: Facilitates easy set-up of security features using a Personal Identification Number (PIN) or other defined methods within the Wi-Fi device. Wi-Fi Protected Setup certifies products which implement technology defined in the Wi-Fi Simple Configuration Technical Specification.
- IBSS with Wi-Fi Protected Setup: Enables ad-hoc connections between devices to complete tasks such as file printing or sharing. Designed to ease setup of connection for devices with limited user interface. IBSS with Wi-Fi Protected Setup certifies products which implement technology defined in the IBSS with Wi-Fi Protected Setup Specification.

Applications and Services

- Miracast: Provides seamless display of content between devices, regardless of brand, without cables or a network connection. Miracast certifies products which implement technology defined in the Wi-Fi Display Technical Specification.
- Voice-Enterprise: Supports a good experience with voice applications over Wi-Fi, enabling fast transitions between access points and providing management. Voice-Enterprise builds on the Voice-Personal certification features.
- Voice-Personal: Voice over Wi-Fi extends beyond interoperability testing to test the performance of products and help ensure that they deliver good voice quality over the Wi-Fi link.
- Wi-Fi Aware: Enables devices in proximity to detect each other by using a power efficient mechanism that establishes a common “heartbeat” and aligns communication windows. Wi-Fi Aware improves on existing proximity offerings by delivering a truly here-and-now contextual awareness solution that empowers users to find services that match their interests. It works well indoors and in dense environments, without requiring a cellular, Wi-Fi, or GPS connection.

Optimization

- TDLS (Tunneled Direct Link Setup): Allows network-connected devices to create a secure, direct link to transfer data more efficiently.
- WMM (Wi-Fi Multimedia): Support for multimedia content over Wi-Fi networks enabling Wi-Fi networks to prioritize traffic generated by different applications using Quality of Service (QoS) mechanisms. WMM certifies products which implement technology defined in the WMM Technical Specification.
- WMM-Admission Control: Enhanced bandwidth management tools to optimize the delivery of voice and other traffic in Wi-Fi networks. WMM-Admission Control certifies products which implement technology defined in the WMM Technical Specification.
- WMM-Power Save: Power savings for multimedia content over Wi-Fi networks. This feature helps conserve battery life while using voice and multimedia applications by managing the time the device spends in sleep mode.

RF Coexistence

- CWG-RF (Converged Wireless Group RF Performance): Developed with CTIA, this is a test program developed for converged devices with both Wi-Fi and cellular technology. The testing provides detailed information about the performance of the Wi-Fi radio in a converged handset, as well as how the cellular and Wi-Fi radios interact with one another. Although this test program is not an element of Wi-Fi certification, completion of the testing is mandatory for Wi-Fi enabled handsets seeking CTIA certification.

Table 8 summarizes Wi-Fi Alliance Certification Programs

Table 8 – Certification Programs

Category	Program	Description/ Technical Specification
Connectivity	Interoperable connectivity	Wi-Fi CERTIFIED a and Wi-Fi CERTIFIED b/g products connectivity
	Advanced Wi-Fi	Wi-Fi CERTIFIED n products connectivity
	Wi-Fi CERTIFIED ac	Test latest version of Wi-Fi in 5 GHz
	Wi-Fi Direct	Wi-Fi Peer-to-Peer Technical Specification
Security	WPA2 (Wi-Fi Protected Access 2)	Wi-Fi wireless network security
	EAP (Extensible Authentication Protocol)	Authentication mechanisms used to validate the identity of network devices in the enterprise
	Protected Management Frames	Extends WPA2 protection to unicast and multicast management action frames
Access	Passpoint	Wi-Fi Alliance Hotspot 2.0 Technical Specification
	Wi-Fi Protected Setup	Wi-Fi Simple Configuration Technical Specification
	IBSS with Wi-Fi Protected Setup	IBSS with Wi-Fi Protected Setup Specification
Applications and Services	Miracast	Wi-Fi Display Technical Specification
	Voice-Enterprise	Builds on the Voice-Personal certification features
	Voice-Personal	Test products deliver good voice quality over the Wi-Fi link
	Wi-Fi Aware	Detect devices in proximity
Optimisation	TDLS (Tunnelled Direct Link Setup.)	Create a secure, direct link to transfer data more efficiently
	WMM (Wi-Fi Multimedia)	WMM Technical Specification
	WMM-Admission Control	Enhanced bandwidth management tools
	WMM-Power Save	Manages the time the device spends in sleep mode
RF Coexistence	CWG-RF	Converged Wireless Group RF Performance Test Plan

1.3.1.2 Wi-Fi Test Suite

Wi-Fi Test Suite is a software platform to support certification program development and device certification.

Non-proprietary components are provided under the ISC License [12] and can be accessed at the Wi-Fi Test Suite open source project on GitHub.

Wi-Fi Alliance members can access the full software package, including proprietary components.

The open source components of Wi-Fi Test Suite are made available to the public in order to help advance the Wi-Fi Alliance mission. Wi-Fi Test Suite embraces technological innovation by being adaptable to all types of unique, diverse, and cutting edge devices. Both Wi-Fi Alliance members and non-members can conduct their own internal testing using the software and tool set provided by the Alliance.

Wi-Fi Test Suite automates testing Wi-Fi components or devices. Wi-Fi Test Suite provides the following services:

- Configure: Automatically configure devices to execute test cases.
- Traffic Generation: Generate traffic streams with specified parameters.
- Test: Execute test scripts by controlling testbed device operation.
- Results Analysis: Determine pass/fail results based on a given test case or script criteria.

Wi-Fi Test Suite accomplishes the services through the following components:

- Control API (CAPI): Command language for device management, test configuration, and test execution within Wi-Fi Test Suite.
- Unified CAPI Console (UCC): Provides the overall control console for Wi-Fi Test Suite.
- Control Agents: A proxy in which a CAPI control command is converted for the device into the device’s native control interface. Access Points (APs), DUTs, sniffers, and Stations (STAs) may require control agents.
- Sniffer: captures and dissects wired and wireless frames, and performs packet analysis.
- Traffic Generator: Produces specific traffic on behalf of Test Bed STA, DUT, or PC Endpoint.
- PC Endpoint: Generates network traffic in support of a particular test plan via the wired Test Network.
- Wi-Fi Alliance certification program test scripts: the Wi-Fi Test Suite specific instantiations of Wi-Fi Alliance test plans.

1.3.2 Open Connectivity Foundation (IoT)

The Open Connectivity Foundation is an organization leading the convergence of IoT technologies. It is dedicated to ensuring secure interoperability for consumers, businesses and industries by delivering standard communications platforms, bridging specifications, open source implementations, and certification programs allowing devices to communicate regardless of form factor, operating system, service provider, transport technology or ecosystem.

OCF arises as the merger of two existing organizations, AllSeen Alliance and Open Interconnect Consortium (OIC) which were developing independent frameworks to deal with IoT, as they realized that IoT can only scale and be truly realized when all “things” are capable of interacting with each other regardless of their underlying technology.

OCF nowadays sponsors both technologies, AllJoyn (initially developed by AllSeen Alliance) and IoTivity (initially developed by OIC). OCF also sponsors the existing certification programs for both technologies.

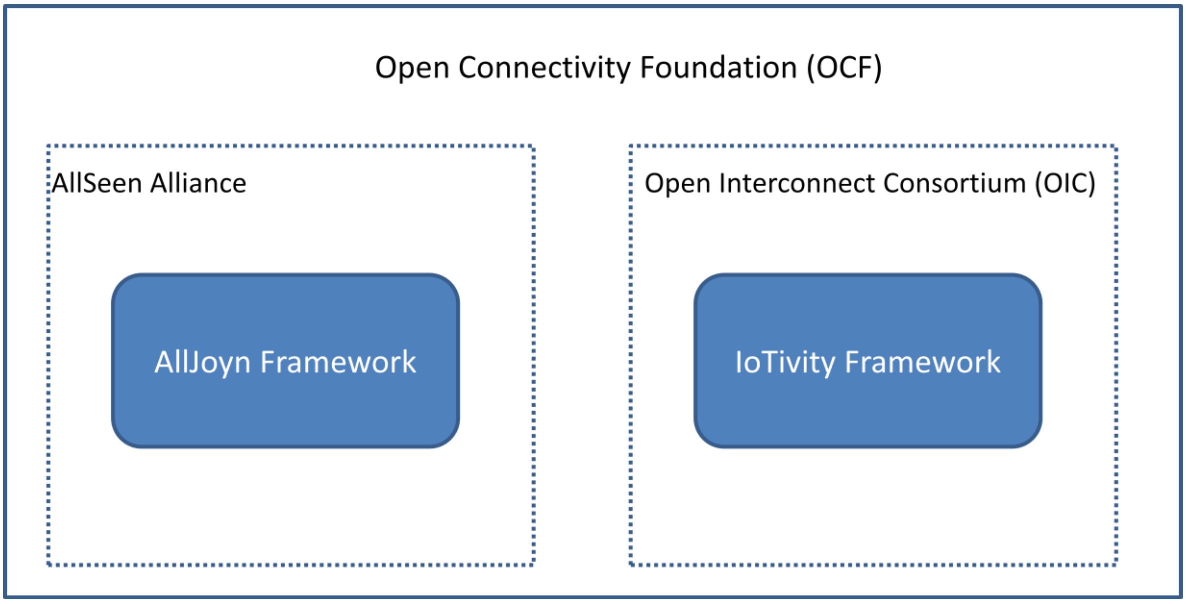

Open Connectivity Foundation (OCF)
AllSeen Alliance
Open Interconnect Consortium (OIC)
AllJoyn Framework
IoTivity Framework

Figure 5 – Open Connectivity Foundation merger

AllSeen Alliance was born as a non-profit organization dedicated to making it easy for devices, appliances and apps to connect to the Internet of Things. AllSeen Alliance enabled industry standard interoperability between products and brands with an open source framework (AllJoyn) that drives intelligent experiences for the Internet of Things. AllSeen Alliance was dissolved after the merger with OCF.

AllJoyn is an open source communication framework that enables IoT device and app interoperability.

Developers can write applications for interoperability regardless of transport layer, manufacturer, and without the need for Internet access (with devices connecting locally). The software has been and will continue to be openly available for developers to download, and runs on popular platforms such as Linux and Linux-based Android, iOS, and Windows, including many other lightweight real-time operating systems.

AllSeen Alliance included more than 200 member companies including leading consumer electronics manufacturers, home appliance makers, automotive companies, cloud providers, enterprise technology companies, innovative start-ups, chipset manufacturers, service providers, retailers and software developers.

Open Interconnect Consortium (OIC), before the OCF merger, was a standard and open source project that delivered interconnectivity technology for developers, manufacturers and end users. OIC's goal was to define the connectivity requirements and to ensure interoperability of the billions of IoT devices, independently of the operating system and network protocol. OIC sponsored IoTivity, an open source reference implementation of the OIC standard specifications.

Though OCF is one of the leading IoT Alliances or consortiums, there are many other IoT Alliances developing their own standards such as Industrial Internet consortium (founded by Intel, IBM, GE, Cisco and AT&T in 2014), the IEEE IoT Initiative (also launched in 2014), the LoRa Alliance (standardizing Low Power Wide Area Networks (LPWAN)) or Open Trust Protocol (including ARM, Symantec and Sprint vendors, developing a protocol to address IoT security challenges).

1.3.2.1 'AllJoyn Certified' Certification Program

The Certification program started by AllSeen Alliance and now taken by OCF for AllJoyn technology is named 'AllJoyn Certified'. It certifies product's compliance with AllJoyn Interface Definitions (AllJoyn specifications [13], [14], [15], [16] and [17]) and ensures Interoperability with other AllJoyn Certified compliant products.

The AllJoyn Certified program testing is composed of conformance testing according to AllJoyn Test Specifications and real world interoperability testing to help OEMs ensure that products work well together.

The AllJoyn Certified program requires the use of approved versions of AllJoyn as identified on the official AllJoyn Certification Matrix: https://allseenalliance.org/compliance.

Table 9 lists the existing AllJoyn certification releases.

Table 9 – AllJoyn Certification Releases

Release	Certification Release	Acceptance date
14.12	14.12.00	2015-05-28
	14.12.00a	
	14.12.00b	
15.04	15.04.00	2015-07-09
	15.04.00a	
	15.04.00b	
15.09	15.09.00	2015-10-30
	15.09.00a	
16.04	16.04.00	2016-06-03
	16.04.00a	
16.10	16.10.00	2017-01-06
	16.10.01	

The Certification Administration Web Tool (CAWT), at https://certify.alljoyn.org is the web used to handle AllJoyn Certified program.

OEMs can start the certification process following the certification guide available at https://certify.alljoyn.org/docs/certification-guide. Certification applications are submitted via web using the CAWT.

Conformance testing is performed using the Certification Test Tool (CTT) developed by AllSeen Alliance, and now maintained by OCF, and based on AllJoyn Test Specifications.

Interoperability testing is performed according to the 'Interoperability Test Procedures' document.

Both, Conformance and Interoperability Test Specifications are available at https://certify.alljoyn.org/docs/alljoyn-certified-test-specifications [19].

Testing is performed by an Authorized Lab. In some specific cases the manufacturer itself may perform the testing and then it will submit the results by using the Certification web tool.

AllJoyn functionalities, such as notifications or configuration, are provided by different services. Table 10 lists the services that can be certified and the related test specifications for conformance testing.

Table 10 – AllJoyn Test Specifications

Core / Service	**Test Specification**
Core	AllJoyn About Feature Test Case Specification
	AllJoyn Events and Actions Feature Test Specification
Control Panel	Control Panel Service Test Case Specification
Notification	Notification Test Case Specification
Onboarding	Onboarding Test Case Specification
Configuration	Configuration Test Case Specification
LSF Lamp Service	LSF Lamp Service Test Case Specification
LSF Lighting Controller	LSF Lighting Controller Test Case Specification
Gateway Agent	Gateway Agent Test Case Specification

1.3.2.1 'OCF Certified' Certification Program

The OCF Certification Program includes conformance testing to ensure robust and secure connectivity.

The certification process is simple. The following steps are performed:

1. The vendor shall become a member of OCF Foundation.
2. The vendor submits a certification application to the OCF Certification Body including:
    - Contact information
    - Product information
    - Product PICS (declaration of product features)

- Authorized Test Laboratory (ATL) where the testing will be performed.

3. The vendor sends the product to the ATL (after approval of the certification application).
4. The ATL will perform the testing according to the Certification Test Plan. After completion it will provide the test logs to the OFC Certification Body.
5. The OCF Certification Body assesses the test results.
6. If the device fulfils the requirements, the vendor receives a Certificate of Conformity.

1.4 Carrier Approvals Private Certification Schemes

Several MNOs (Mobile Network Operators), also known as wireless Carriers, will acquire cellular devices that have gained regulatory certification and GCF and/or PTCRB certification without additional requirements. However, there are MNOs that require some additional testing to be performed to confirm that those cellular devices will behave correctly on their own infrastructures.

Accordingly, these carriers have launched their own qualifications programs (also called approval, homologation, device acceptance or certification programs). The MNOs' concern is that the device will play smoothly with their own networking equipment and with their specific configurations, behaving predictably and coexisting with the other consumer and industrial devices that share their network.

Each MNO has its own unique requirements. Requirements may change over time, so it is important that OEMs confirm with the MNOs qualification services a product is going to be launched before starting product development. Operators' information may dramatically affect the business case.

Part of the testing required by the MNOs is normally performed at a third party test lab approved by the MNO to perform the testing. There may also be homologation testing required that needs to be performed by the MNO to ensure a device is operating properly on its network.

TRP/TIS performance is an example of specific requirement that is commonly requested by many operators. Sometimes the operators will accept PTCRB TRP/TIS testing but they will impose additional requirements on the results obtained.

1.4.1 Telefónica

Telefónica is main Spanish mobile network operator, present in 21 countries and with an average of 125,000 employees and about 350 million customers.

1.4.1.1 Telefónica terminals homologation program

Telefónica terminal qualification program is a process divided in several steps or stages. Each stage has its own technical gate to decide if a device is approved and the device can continue to the next stage or if the product is withdrawn.

Each gate uses a set of criteria to evaluate whether to progress to the next stage

The Telefónica homologation program comprises 3 gates:

- Selection gate.
- Test Entry gate.
- Approval gate.

In the Selection gate, the Gating criteria define the minimum requirements for a device to pass a gate. The requirements included in the Gating criteria are mandatory and not supporting these requirements will prevent those devices from being selected by Telefónica.

For example, some frequency bands will be required depending on the country where the device is going to be launched. There are also some global requirements such as support of Circuit Switched Fallback (CSFB) or the requirement that LTE devices shall support at least LTE UE Category 3, that is, support of 100 Mbps downlink and 50 Mbps Uplink, to ensure high data throughputs.

Devices are also grouped in different types according to their characteristics. Device types include chipsets, datacards or USB modems, laptops, netbooks, M2M devices (with and without display), mobile phones, modules, etc. Requirements or features to be supported by different types of devices may be different.

Additionally, Telefónica defines the selection influential criteria. The requirements included in these criteria improve the device performance. Not supporting these requirements may mean that the device will not be selected. Support of most of these requirements will increase the device selection options. Support of VoLTE and Wi-Fi at 5 GHz are examples of influential requirements.

Test Entry Gating Criteria defines the requirements for devices overcoming the Selection gate. The device manufacturer is required to meet each of these criteria before the qualification process can start. Part of these requirements consists in providing devices and accessories for local and global testing, validating device provided documentation, etc.

After passing the Test Entry Gating Criteria, the qualification process itself starts. The Approval gate has two different types of criteria: the approval gating criteria and the Approval Key criteria.

The Approval Gating criteria are the minimum criteria that must be met for device Approval to be awarded. GCF declaration and CE certificate are some of the gating criteria for Europe. Antenna performance is a requirement for all Telefónica networks.

Approval Key criteria comprise non mandatory but highly recommended requirements. These requirements are highly desirable to be supported and the support of these features will be valued by Telefónica and will speed up the qualification process. Approval Key criteria contain requirements such as having Wi-Fi or Bluetooth certificates or a battery life testing certificate.

Telefónica has developed its own Test Specification, TTS (Telefónica Test Specification) for qualifying products. TTS defines a set of tests that any OEM device needs to successfully pass in order to be able to sell its device to Telefónica. TTS is an extensive document including several thousands of individual requirements to be passed by the terminals and the corresponding tests to verify the requirements.

These tests are grouped according to functionalities supported by the device, like AT commands, Bluetooth, email, GPRS, GSM, SMS/MMS, Wi-Fi, etc.

Telefónica names the complete list of tests to be executed on a terminal the 'Acceptance Test Plan'. This Acceptance Test Plan consists of a set of test cases defined in the TTS. TTS is being updated continuously as the new improvements and technologies appear.

Each Telefónica local country subsidiary has been using its own 'Acceptance Test Plan' but recently Telefónica has harmonized the requirements among the subsidiaries (mainly in LATAM), improving the quality of the process and the Time To Market.

1.4.2 AT&T

AT&T Inc. is an American telecommunications corporation, and one of the largest providers of fixed and mobile telephony in the world. Its main business is located in the United States. AT&T delivers advanced mobile services, next-generation TV, high-speed Internet and smart solutions for people and businesses.

1.4.2.1 AT&T Acceptance program

AT&T develops a 'Device requirements' document where the carrier lists the requirements for devices looking for AT&T acceptance. Those requirements are set for all type of devices from voice terminals to PC cards.

AT&T provides these requirements documentation to possible device suppliers so they understand properly AT&T policy for product acceptance and core technical requirements.

Every product submitted to AT&T for consideration must be accompanied by a completed Handset Specification Compliance workbook where the supplier compliance with AT&T's requirements is shown. AT&T will deliver these proprietary AT&T certification documents to be completed and returned (after appropriate NDA signature). The information to be fulfilled is extensive and provides exhaustive detail about the device functionality. The information to be fulfilled depends on the type of product and the business segment.

Every AT&T's requirement includes a priority status to indicate if the requirement is:

- Required: Mandatory to be supported.
- Preferred: The support of the requirement is not mandatory but its support is valued by AT&T.
- Informational: The supplier will provide this information but AT&T does not have a preference in the support of the functionality.

AT&T has specific requirements for certain technologies and certain bands. For example, LTE devices are expected to support the four bands currently available in AT&T's network (LTE bands 2, 4, 5 and 17). LTE data-only devices are expected to support at minimum EDGE quad-band (850, 900, 1800 and 1900 MHz) and UMTS tri-band (850, 1900 and 2100 MHz) in addition to LTE quad-band. In any case, as new bands are expected in the near future, these requirements are expected to change.

Once that a product submitted to AT&T for consideration has been accepted, the manufacturer or vendor needs to enter its product through the so called 'AT&T Terminal Unit & Accessory Technical Acceptance' process.

This Technical Acceptance process consists of two elements.

- Documentation: Such as Lab Entry Criteria documentation, Test results and PTCRB Certification.
- Testing: Various types of AT&T performed testing including lab testing and field testing.

AT&T requires devices to pass PTCRB certification, before starting the AT&T acceptance program. AT&T adds Pass/Fail criteria to the TIS/TRP minimum performance results obtained during PTCRB certification process. AT&T’s specifications are more than 500 pages long and devices need to pass all applicable test cases of the specification.

1.5 Certification of Apps

Nowadays, App Certification is a requirement for publication on the main mobile app stores.

The concept of mobile app certification for different mobile operating systems has been around for a number of years. Initially some of the test and validation of these schemes were carried out by approved test vendors that would test versions of the application that would, subject to achieving the desired approval, receive a validation mark and signature that would be necessary for a mobile app to be submitted to certain mobile app store or mobile operator app store. Examples of these schemes include:

- Java Verified [25].
- Symbian Signed [26].
- Microsoft Mobile2Market [27].

An alternative approach used by some app store providers is where the app store provider carries out all the necessary validation work itself. This could be to have more control over all aspect of the submission and approval option, or possibly to make it easier for app developers to have a more streamlined experience in submitting apps that meet the required guidelines. Examples of these types of programmes include:

- Apple.
- QUALCOMM BREW.
- Blackberry.

Many of these ecosystems above have, for a number of reasons, not lasted to be major players in the mobile application ecosystem. According to recent Gartner report [19], the main mobile operating systems are predominantly Android (Google and non-Google ecosystems) and Apple iOS.

Table 11 – Operating Systems Market Share (Gartner report)

Operating System	**4Q16 Units**	**4Q16 Market Share (%)**	**4Q15 Units**	**4Q15 Market Share (%)**
Android	352,669.9	81.7	325,394.4	80.7
iOS	77,038.9	17.9	71,525.9	17.7
Windows	1,092.2	0.3	4,395.0	1.1
BlackBerry	207.9	0.0	906.9	0.2
Other OS	530.4	0.1	887.3	0.2
Total	**431,539.3**	**100.0**	**403,109.4**	**100.0**

This section focuses on aspects relating to the major App Store Providers (Google, Apple and Microsoft). Although there are multiple Android based app stores, particularly in China, for simplicity, Google Play is the focus of the main information presented in this section. The major App Store Certification or approval schemes examined are listed in Table 12:

Table 12 – Test Specifications

Organisation	**Test Specification**
Apple	Apple App Store App Review [28]
Google	Google Play Store App Guidelines [29]
Microsoft	Windows App Certification [30]

1.5.1 App Certification Review Criteria

The following are important criteria by which applications are reviewed on the major app stores:

- Privacy Policy – each application requires a privacy policy to clearly indicate what data is being collected, whom the data is shared with (what third parties) and how the data will be used.
- Security – this can include checking for malware and also ensuring that app permissions are reasonable. Guidelines include recommendations of authentication, securing data at rest and in transit. In the case of Microsoft and Apple there are clear guidelines that developers should avoid the use of internal or private APIs.
- User Interface Guidelines – ensuring that the User Interface for applications is usable for end users and follows the usability guidelines for each platform. Each platform aims to have a level of consistency between apps to improve usability for users by using patterns of navigation and content presentation. Google Play [20] suggests guidelines for developers, however Apple and Microsoft [21] strongly enforce adherence to these guidelines or applications will not be approved. A key aspect of the user interface is how the application will display on multiple screen sizes, resolutions and screen orientations. Android in particular is quite difficult to support in this regard, due to the wide diversity of devices on the market. The main mobile operating system providers also support applications that target multiple types of device such as TV, car and wearable.
- Content Guidelines – App content should be appropriate for the market and age of the user. This content can vary depending on local laws and cultural expectations and the age of the target user. Particular care needs to be taken for applications that are used by children.
- Accessibility – how applications can be used by users with disabilities or reduce capabilities. Common approaches could be to connect a Braille display device over Bluetooth or to use spoken interface components, this requires that labels and icons have appropriate spoken meaningful names.
- Legal – verifying if an app is a clone of an already existing app, if there is trademark infringement and if the app complies to all relevant regulations and laws in the territories where the app is available. Particular care needs to be taken when the application requires payment.
- Localization - applications must be localized for all languages that it supports, this will include text, but also cultural symbols and iconography.

- Performance – Examining the performance of the application during foreground and background execution. This could include examining the CPU and memory usage of the application, especially in background mode and how the app manages resources when they are not immediately needed. One common area considered here is for apps that use location to track user movements.
- Network Usage – This is an important area that examines the frequency and volume of connectivity and the architecture, for example does the app continuously poll for updates, or does it make use of push notification architectures.

1.5.2 App Certification Tool Support

The Apps Quality Alliance (AQuA) is an independent organisation that publishes guidelines on improving quality. They have a number of publications in the area of improving overall app quality, regardless of platform. One of their initiatives has been to create a Performance Testing Criteria [22], and selected AT&T Application Resource Optimizer (ARO) [23] as a tool help developers to optimise app performance.

The Mobile Ecosystem Forum (MEC) has created a Privacy Policy generation tool [31] that can assist developers to generate a suitable privacy policy.

A number of mobile development tools have built-in tools to assist developers in monitoring device performance during application execution and also to preview what their applications will look like on different devices. In practice, these tools should be used in addition to testing and monitoring on real devices, as emulators and preview tools are different from real-world devices.

Microsoft and Apple have functions integrated into their development tools that can assist developers in submitting their apps by providing integration with app store submission APIs and for validating certain criteria during submission, before being passed to human and automated analysis.

1.6 Summary of certification schemes research

The research performed on the existing certification schemes has brought the following conclusions:

- Regulatory certification schemes are related to devices and there is no regulatory requirement for Apps. These schemes focus on health requirements and on RF/EMC requirements to verify that the device is not going to be harmful to other devices or to the telecommunication networks. They provide a limited warranty of quality, interoperability, safety, immunity and/or efficiency in the use of some limited resources.
- Cellular Industry certification schemes cover a large part of the testing gap of the regulatory certification schemes. They verify thoroughly the protocol behaviour of the device, verifying that the product provides the expected answer under hundreds of defined scenarios. They also verify that the RF signals are transmitted and received according to defined (3GPP) standards, assuring that the telecom service is going to be provided also under rough radio scenarios.
- Smart phones are introducing additional technologies, such as Wi-Fi, Bluetooth or NFC, that may imply additional regulatory requirements and new specific certification programs for those technologies.
- Carrier certification schemes perform a deeper testing to verify the behaviour of the device on the operator networks. They also perform some performance testing to characterize devices. However these results are confidential inside the network operator and the results are not disclosed to the marked. Network operators in general do not specifically test Apps.
- Mobile Apps certification is currently a mobile apps stores requirement. Android and iOS are the most important App stores providers covering over 99% market share. Main criteria by which applications are reviewed are security, privacy policy, user interface, contents, accessibility, localization, performance, network resources usage and legal issues.

Our research has identified that there is not a global performance testing that allow users compare products to determine how these products will behave according to relevant parameters such as consumption of energy or performance under limited network conditions. There is here a gap that TRIANGLE mark intends to cover.

In the apps world, it has been pointed out that there is no global certification scheme taking the lead of the market. There are a few schemes but none of them has a global leadership. TRIANGLE mark intends to position itself in the mobile (wireless) apps world.

From the certification process point of view, successful certification schemes typically use third party independent testing laboratories to perform the testing and assure the validity of the testing results. Testing costs lay on products’ vendors and manufacturers, who obtain a certificate that shows their product covers market requirements. Most schemes trust on industry experts, usually named Certification Bodies, which assess the testing results and verify whether the certification scheme’s requirements have been fully covered by the testing and the certification may be granted. Certification bodies also normally take the role of guiding users in the certification process and resolving disputes.

TRIANGLE has also verified that in order to be successful, a certification scheme needs to be known, recognized and accepted by the market. Technically outstanding certification schemes do not bring value to the market if they are not widely used. Becoming part of an already successful certification scheme would provide a relevant advantage to get its place in the market.

TRIANGLE is holding discussions with the GCF global mobile certification scheme to try to integrate TRIANGLE mark into GCF certification requirements.

2 Certification Scheme

2.1 Introduction

The primary objective of the TRIANGLE project is to promote the testing and benchmarking of mobile applications and devices as the industry moves towards 5G and to provide a pathway towards certification in order to support qualified apps and mobile developments using FIRE testbeds as testing framework.

TRIANGLE mark certification is based on performance testing.

Conformance testing, a testing performed by a Test System to verify the compliance of a product, according to certain standards, according to a Pass/Fail criteria, is not part of TRIANGLE certification. Devices undergoing TRIANGLE certification are expected to have been already certified according to industry main certification schemes, being the TRIANGLE objective, to benchmark the products according to their performance.

Interoperability testing is also not part of TRIANGLE certification.

The objective of this section is to define the certification scheme to be used to certify products according to TRIANGLE requirements.

The starting point to define this new certification scheme is to understand existing certification schemes for the products under the scope of the project. It is very important to understand the commonalities and differences and any possible overlap between the existing schemes.

The objective of TRIANGLE certification is to verify the performance of a mobile app or a device.

TRIANGLE certification consist on a set of test cases configured according to defined use cases and under specific test scenarios, that determine the performance of the device or application under test for a list of key performance indicators (KPIs).

The evaluation of the application or device performance is divided into domains. Each domain focuses on a special characteristic such as energy consumption or quality of experience.

The TRIANGLE mark provides a score for every domain evaluated in the application or device, as well as a global score. The mark's objective is to create a simple mobile applications and devices evaluation or scoring to provide final users a clear idea of that application or device behaviour.

The TRIANGLE mark allows that totally different applications or devices, being used in different use cases, can be assessed in an equivalent way, taking into account their performance in the domains specified by the TRIANGLE project.

2.2 What is under certification

TRIANGLE certification covers the products listed in this section.

2.2.1 Apps

An App is computer software, specifically developed to be used for mobile devices.

TRIANGLE certification program initially will only cover certification of Apps developed for Android and iOS operating systems.

Only apps that make use of 5G or pre-5G technology may obtain the TRIANGLE mark.

Apps will fall into one of the following use cases: virtual reality, gaming, augmented reality, content distribution streaming services, live streaming services, social networking, high speed internet, patient monitoring and emergency services. Nevertheless, additional use cases are expected to be added in the future.

Following software elements are not under the scope of TRIANGLE mark certification:

- PC Applications.
- Software running on servers.
- Applications that do not use 5G or pre-5G technologies.

2.2.2 Mobile devices

Mobile devices are computing devices, small enough to hold and operate in the hand. Mobile devices with Android and iOS operating systems can initially be certified to obtain the TRIANGLE mark. In the future other OS may also be supported.

Mobile devices must be able to run Android and iOS Apps (according to their OS).

Mobile devices will have a display screen and real or virtual keyboard.

Certifiable mobile devices must support 5G or pre-5G technology.

2.2.3 IoT devices

From TRIANGLE perspective, an IoT device is an electronic device, to be connected to other devices or systems through a 5G or pre-5G network.

An IoT device can operate to some extent interactively and autonomously.

In a first stage, following types of IoT devices can be certified to obtain TRIANGLE mark:

- IoT devices for smart metering and sensing/recording.
- IoT devices working in Smart Grids environment such as smart meters, smart appliances, etc.
- IoT devices to be used as part of Connected Vehicle systems.

2.3 Roles and Actors

The actors participating in the TRIANGLE mark certification process are:

2.3.1 Applicant

An applicant is any Application Developer, Device manufacturer, vendor, etc., requesting to obtain TRIANGLE mark for its product.

The applicant is responsible for:

- Creating TRIANGLE mark Certification Applications.
- Providing product documentation (including lists of features, supported use cases (ICS), IXIT, and any relevant applicant declaration.
- Selecting one Test Lab to perform testing.
- Providing Apps or, in the case of devices, required samples with ancillaries to the Test Lab to perform the testing.

2.3.2 3rd party Test Lab

Entity authorized by TRIANGLE to perform certification testing.

During the first two years after TRIANGLE mark is released, the Test Lab will not have any certification accreditation requirements. After this period, TRIANGLE Test Lab will need to be ISO 17025 accredited. This two years period will allow Test Labs start certification activities immediately and at the same time it will give enough time to labs to get required accreditation.

The 3rd party Test Lab (or just Test Lab) has the following responsibilities:

Test Plan generation: The Test Lab is responsible for producing the Test Plan (complete list of test cases to be performed to obtain certification) by means of using a TRIANGLE validated testbed, based on the product’s features, supported use cases and scenarios (as provided by the applicant in the product’s ICS statement.

Testing execution: The Test Lab performs testing by using a TRIANGLE validated testbed as technical evidence of TRIANGLE certification program.

Testing will be performed in a reliable, mature and repetitive way.

Test Report generation: The Test Lab issues a Test Report when all testing is completed.

Submission of documents: The Test Lab submits formally all testing evidences and any additional required document to the Certification Body for assessment.

Testbed maintenance: The Test Lab will hold and maintain TRIANGLE testbeds according to latest TRIANGLE requirements.

2.3.3 Certification Body

The Certification Body is an entity (person or group) with the following responsibilities:

- **Test Plan assessment**: The Certification Body assesses the certification Test Plan to verify that all the applicable test cases, and only those ones, are added to it.
- **Certification documentation assessment:** The Certification Body assesses the correctness and completeness of the product documentation submitted for certification.
- **Certification issues assessment**: The Certification Body will receive notifications from device vendors and Apps developers related to issues with TRIANGLE validated testbeds and/or TRIANGLE test specifications that may affect the certification of a product. The Certification Body will verify the existence of such issues and if they exist, it will take the required actions to get them solved. Issues with the testbed or Test Specifications will not delay the certification of a product.
- **Supply Certificate of Conformity** for products that have completed the TRIANGLE certification process and that have filled the certification requirements.

TRIANGLE will approve and designate individuals to take the Certification Body role. It is expected that Test Lab companies will propose one or more experts to become TRIANGLE certification bodies.

2.4 Types of certification

Following types of certification in the TRIANGLE certification program:

New Product

New Product Certification is the initial certification of a product.

Product Update

Product Update Certification is the certification of a new release of an already certified product. The newer release of the product has at least a modification of any of its software and/or hardware components.

Product Re-Branding Certification

Product Rebranding Certification is the certification of a product where the only changes from an already certified product are related to the branding of the product, including cosmetics changes of the product.

2.5 Types of testing

The primary objective of the TRIANGLE project is to promote the testing and benchmarking of mobile applications and devices as the industry moves towards 5G and to provide a pathway towards certification in order to support qualified apps and mobile developments using FIRE testbeds as testing framework.

TRIANGLE mark certification is based on performance testing.

Conformance testing, a testing performed by a Test System to verify the compliance of a product, according to certain standards, according to a Pass/Fail criteria, is not part of TRIANGLE certification. Devices undergoing TRIANGLE certification are expected to have been already certified according to industry main certification schemes, being the TRIANGLE objective, to benchmark the products according to their performance.

Interoperability testing is also not part of TRIANGLE certification.

2.5.1 Performance testing

The objective of TRIANGLE certification is to verify the performance of a mobile app or a device.

TRIANGLE certification consist on a set of test cases configured according to defined use cases and under specific test scenarios, that determine the performance of the device or application under test for a list of key performance indicators (KPIs).

The evaluation of the application or device performance is divided into domains. Each domain focuses on a special characteristic such as energy consumption or quality of experience.

The TRIANGLE mark provides a score for every domain evaluated in the application or device, as well as a global score. The mark’s objective is to create a simple mobile applications and devices evaluation or scoring to provide final users a clear idea of that application or device behaviour.

The TRIANGLE mark allows that totally different applications or devices, being used in different use cases, can be assessed in an equivalent way, taking into account their performance in the domains specified by the TRIANGLE project.

2.6 Processes

2.6.1 The certification process

TRIANGLE certification process starts when an applicant requests to certify a product by sending a filled certification application form to one of the approved TRIANGLE Certification Bodies.

The Certification Application Form is available in Annex A of this document.

The applicant will also select a Test Lab to perform the testing and as agreed with the Test Lab will send the required samples (in the case of device certification) or will provide the App for testing.

The selected Certification Body will be responsible for guiding the applicant through the whole certification process.

The applicant will send the Test Lab, all the required documentation to certify its product.

- Copy of the Certification Application Form.
- List of features, use cases and scenarios supported by the product (ICS tables).
- Product user manual or brief description explaining how to use the product for testing purposes.

The Test Lab will generate a Test Plan, i.e., the list of test cases to be executed to certify the product, according to the features supported by the product.

The Test Plan is obtained as the list of the product applicable test cases from the Test Case Reference List (TCRL), i.e. the complete list of test cases required by TRIANGLE for product certification.

The Certification Body will assess the Test Plan to verify its correctness and completeness.

Once the Test Plan is agreed, the Test Lab will start testing on it.

After finishing the execution of all the test cases in the Test Plan, the Test Lab will generate a Test Report where results of the testing are listed.

The Certification Body will assess the Test Report together with the testing evidences generated by the testbed and will verify whether all certification requirements are met.

When all certification requirements are met the Certification Body will issue the TRIANGLE mark for the product tested, completing the certification of the product.

The product information will be added to a list of TRIANGLE certified products.

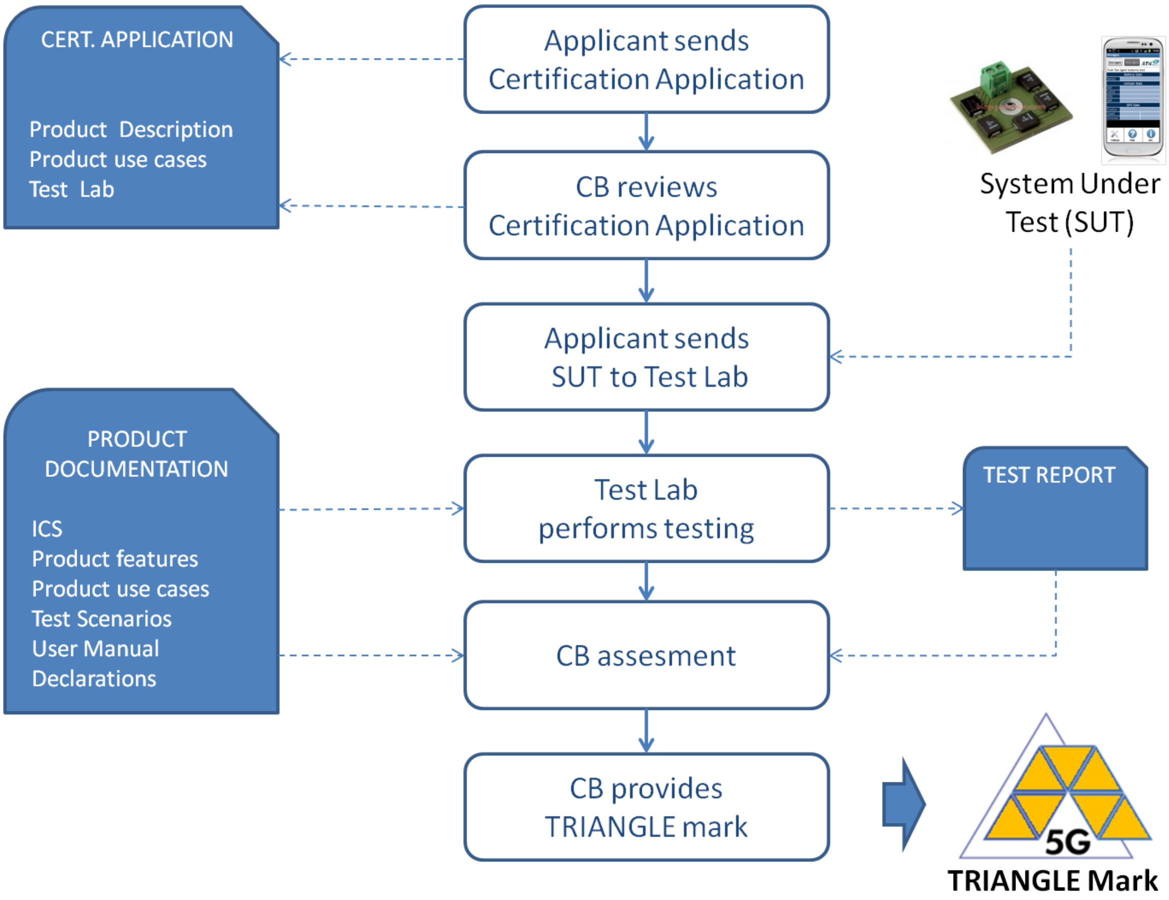


Figure 6 – TRIANGLE Certification process

2.6.2 Handling issues with TRIANGLE validated testbeds and TRIANGLE Test Specifications

During the certification process, it could happen that one (or more) of the certification requirements cannot be demonstrated due to a possible issue with one or more TRIANGLE validated testbed or with any of the TRIANGLE Test Specifications.

TRIANGLE defines a procedure to handle these issues and prevent that one of these issues stops or delays the certification process unnecessarily.

An Issue with the test specification happens when an applicant or Test Lab understands that the definition of a test case, or the test procedure defined to verify the test objective is not correct.

An issue with TRIANGLE validated testbed happens when the TRIANGLE testbed does not implement correctly or completely a test case as it is defined in the corresponding Test Specification.

Handling issues process

When an applicant or Test Lab identifies a possible Test Specification or TRIANGLE testbed issue, they will notify it to the Certification Body responsible for the certification process of the ongoing product certification.

In cases where an issue is identified, but it is not related to any product certification, the applicant or Test Lab may notify it to any of the TRIANGLE approved Certification Bodies.

The Certification Body will review the issue information and determine if the issue may be real. The CB will contact the TRIANGLE teams responsible of the Test Specifications definition and/or TRIANGLE testbed development team if it needs any clarification regarding the issue.

If it is agreed that the issue is real; the certification requirement may need to be removed totally or partially (if the issue only affects a restricted number of products or cases). If this is the case, the TRIANGLE Test Case Reference List (TCRL) will be updated accordingly.

The updated TCRL will become effective immediately.

The Certification Body will also start the required procedures to get the issue solved and, if possible, will get a time estimation for the implementation of the solution.

2.6.3 Certification Violations

TRIANGLE defines a process to handle possible certification violation.

The situations detailed below are identified as certification violations:

- A device vendor distributes a mobile device that does not have the TRIANGLE mark, but the vendor sells the product indicating it is TRIANGLE certified (e.g. using the TRIANGLE mark label.
- An App developer supplies an App including a TRIANGLE mark logo or any other reference to TRIANGLE mark without having certified the App.
- A device vendor or App developer supplies its certified product but showing a different global score and/or a domain score different from the product score obtained during product certification in the Test Lab.
- A device vendor or App developer makes changes to a certified product that affect the TRIANGLE mark certification requirements, and the device vendor or App developer does not certify the new version of the product.
- A device vendor provides samples or the App developer provides an App to the Test Lab for certification with one or more HW/SW changes compared to the product that is going to be commercialized and without informing the Certification Body.
- Product features, use cases and/or test scenarios (ICS tables) provided for certification do not match the product real information in order to ease or skip certification testing.

Identifying Violations

When an apparent certification violation is identified, it shall be notified to TRIANGLE.

The identifying party shall provide all the available details and documentation about the suspected certification violation. They identifying party may also provide comments about the impact caused by the certification violation from its point of view.

TRIANGLE (or an entity assigned by TRIANGLE, such as a Certification Body) shall assess the documentation. If TRIANGLE understands that there is rational evidence that a certification violation may be happening, TRIANGLE shall get in contact with the vendor/developer responsible of the apparent certification violation and will ask for clarification on the case.

After discussion with the vendor/developer, TRIANGLE will determine whether the certification violation is real or not, and will decide whether to place the offending OEM on probation for a period of time. If TRIANGLE determines that the certification violation is real, it may decide to set the vendor/developer's product on probation.

A vendor/developer will not be responsible for certification violations due to the Test Lab or Certification Body errors or omissions when certifying its product.

Probation

TRIANGLE may audit products set on probation at its own discretion. The audit may include testing performed in a TRIANGLE Test Lab. The vendor/developer will be responsible for any cost consequence of the auditing activities and will pay for all those costs.

TRIANGLE may remove certifications of products that

- Fail to comply with certification requirements during the audit, or
- Obtain a global or any domain score significantly below the score obtained during certification.
- The vendor/developer does not allow performing product's audit or refuse to pay the audit's costs.

A product certification will be removed in any case, after three certification violations of that product.

Resolving Violations

Vendors will urgently stop the shipment of devices with a certification violation. Vendors will also provide a way to solve the certification violation.

App developers will stop immediately distributing their app and will remove or disable any location from where the app may be downloaded.

3 Test Specifications

3.1 General concepts

In order to complete TRIANGLE certification, a device or application implementation needs to be evaluated under a set of certification requirements.

The different certification requirements are verified by the execution of individual test cases. The complete description of the test cases is defined in a set of Test Specifications.

A different Test Specification will be created for all the domains identified in TRIANGLE project to include all the test cases required to evaluate a specific domain. Table 13 lists the domains identified for TRIANGLE certification and the domains applicable for the defined SUTs.

Table 13 – TRIANGLE domains

Domain	**Application**	**Mobile device**	**IoT device**
Reliability	Yes		Yes
Network Resources usage	Yes		
User Experience	Yes		
Device Resources usage	Yes		
Network Adaptation	Yes		Yes
Energy Consumption	Yes	Yes	Yes
Data Performance		Yes	Yes
Radio Performance		Yes	Yes
User Experience with Reference Apps		Yes	

TRIANGLE mark covers different Systems Under Test (SUT): Applications and Devices. Devices can be also subcategorized into mobile devices and IoT devices. IoT devices can also be classified as Grid Operated IoT devices and battery powered IoT devices. Additionally, battery powered IoT devices can be classified as Short battery duration IoT (SL-IoT) devices and Long battery duration IoT (LL-IoT) devices.

Figure 7 shows the classification of IoT devices.

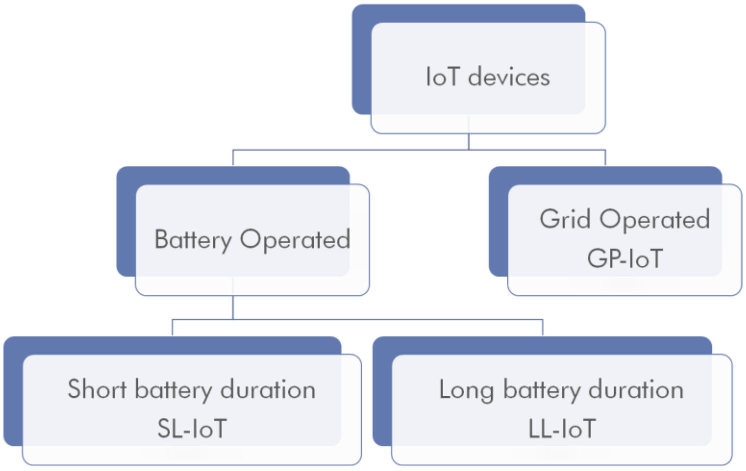


Figure 7 – Types of IoT devices

It is also proposed to create separated Test Specifications for different SUT. Accordingly, the Test Specifications listed in the Table 14 shall be defined.

Table 14 – TRIANGLE Test Specifications

System under Test	**Domain**	**Identifier**	**Test Specification**
Application	Reliability	REL	Applications Reliability Test Specifications
Application	Network Resources usage	NWR	Applications Network Resources usage
Application	User Experience	AUE	Applications User Experience
Application	Device Resources usage	RES	Applications Device Resources usage
Application	Network Adaptation	NWA	Applications Network Adaptation
Application	Energy Consumption	AEC	Applications Energy Consumption
Mobile device	Data Performance	QOS	Mobile devices Data Performance
Mobile device	Radio Performance	RFP	Mobile devices Radio Performance
Mobile device	Energy Consumption	DEC	Mobile devices Energy Consumption
Mobile device	User Experience with reference apps	DRA	Mobile devices User Experience with reference apps
IoT device	Reliability	IDR	IoT Devices Reliability
IoT device	Network Adaptation	INA	IoT Devices Network Adaptation
IoT device	Radio Performance	IRP	IoT Devices Radio Performance
IoT device	Data Performance	IDP	IoT Devices Data Performance
IoT device	Energy Consumption	IEC	IoT Devices Energy Consumption

Test Specification test cases are organized by use cases (as shown in Table 16).

Table 15 shows the use cases that have been defined for TRIANGLE Certification and the contents of testing that are applicable to the use cases:

Table 15 – TRIANGLE Use cases

Identifier	Use Case	Application	Mobile device	IoT Device
VR	Virtual Reality	Yes	Yes	
GA	Gaming	Yes	Yes	
AR	Augmented Reality	Yes	Yes	
CS	Content Distribution Streaming Services	Yes	Yes	
LS	Live Streaming Services	Yes	Yes	
SN	Social Networking	Yes	Yes	
HS	High Speed Internet	Yes	Yes	
PM	Patient Monitoring		Yes	Yes
ES	Emergency Services		Yes	Yes
SM	Smart Metering		Yes	Yes
SG	Smart Grids		Yes	Yes
CV	Connected Vehicles		Yes	Yes

Table 16 shows the use cases applicable to the defined test specifications.

Table 16 – TRIANGLE Use cases applicability per Test Specification

	Virtual Reality	Gaming	Augmented Reality	Content Distribution Streaming Services	Live Streaming Services	Social Networking	High Speed Internet	Patient Monitoring	Emergency Services	Smart Metering	Smart Grids	Connected Vehicles
TS ID	***VR***	***GA***	***AR***	***CS***	***LS***	***SN***	***HS***	***PM***	***ES***	***SM***	***SG***	***CV***
REL	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩			
NWR	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩			
AUE	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩			
RES	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩			
NWA	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩			
AEC	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩			
DEC	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
QOS	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
RFP	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
DRA	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
IDR								🟦	🟦	🟦	🟦	🟦
INA								🟦	🟦	🟦	🟦	🟦
IRP								🟦	🟦	🟦	🟦	🟦
IDP								🟦	🟦	🟦	🟦	🟦
LDP								🟦	🟦	🟦	🟦	🟦
LEC								🟦	🟦	🟦	🟦	🟦
GEC								🟦	🟦	🟦	🟦	🟦
SEC								🟦	🟦	🟦	🟦	🟦

Additionally, each test case will be executed for all the scenarios that are relevant to the SUT and that specific test case.

Table 17 (defined in D2.1) lists the scenarios identified for TRIANGLE certification.

Table 17 – TRIANGLE Scenarios

Scenario	**Scenario Description**	**Sub-Scenario**	**Sub-scenario Description**
UR	Urban	OF	Office
		PE	Pedestrian
		DN	Driving, Normal
		DT	Driving, Traffic jam
		DE	Driving, Emergency driving
		IB	Internet Cafe, Busy hours
		IO	Internet Cafe, Off-Peak
SU	Sub-Urban	FE	Festival
		ST	Stadium
		SB	Shopping Mall, Busy hours
		SO	Shopping Mall, Off-Peak
HS	High Speed Train	RE	Relay
		DP	Direct Passenger connections
IT	Internet of Things	WA	Warehouse
		OS	Outdoor sensors
		HS	Home sensors

Annex B of this document indicates the scenarios applicable to the different use cases defined by TRIANGLE.

3.2 Test Specification contents

Every Test specification will contain the sections described in Table 18:

Table 18 – TRIANGLE Test Specifications sections

Section	Title	Description
1	Introduction	This section shall provide an overview of the entire document and a description of the scope of the Test Specification.
1.1	Purpose	This section *shall* describe the purpose of this document. The section should also specify the intended readership of the document.
1.2	Scope of testing	*This section shall summarise the features of the devices and applications to be tested.*
1.3	Definitions, Acronyms and Abbreviations	This section shall define all terms, acronyms and abbreviations used in this document.
1.4	References	This section shall provide a complete list of all the applicable and reference documents, indicating title, author and date.
2	General Test conditions	This section shall include the generic test conditions where the test cases will be executed.
3	Test cases	This section shall include the complete description of the test cases identified as part of the certification requirement. The description shall be according to section 3.3.
3.n	Use cases	Section 3 may be divided into several sub-sections to group test cases according to the different applicable use cases
4	Test cases applicability	This chapter shall contain the test cases applicability condition according to the ICS defined D2.2 Appendix 2. ICS/IXIT.

3.3 Test naming convention

This section defines the naming convention to create the reference associated to each test case.

The proposal to name test cases references is the following one:

Generic Test case name: ***TSI/UC//XXX***

Test case name with specific scenario: ***TSI/UC/XXX[SC/SS]***

Where:

TSI: Test Specification Identifier, as defined in table 13.

UC: TRIANGLE 5G Use case as defined in table 14.

SC: TRIANGLE Scenario as defined in table 16.

SS: Sub-Scenario belonging to the SC scenario as defined in table 16.

XXX: Test case number

3.4 Test case description

This section describes the required contents to define a test case to be included in section 3 of a Test Specification (as defined in Table 18).

The definition of a test case will include the following fields:

Test case Identifier: According to Test Naming convention

Test case Title: Name of the test case

Test case objective: Describe the test case and its objective

Test case applicability: Define devices / application that have to execute the test case according to the ICS values.

Test case Initial Conditions: Initial configuration and state of the entities taking part in the test case

Test case Steps: Steps to perform the test case

Measurements: Measurements that are performed in the test case execution

4 References

[1] DIRECTIVE 1999/5/EC of the European Parliament and of the council. [Online]. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0005.

[2] DIRECTIVE 2014/53/EU of the European Parliament and of the council. [Online]. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053

[3] Wi-Fi Alliance. Certification Programs. [Online]. http://www.wi-fi.org/certification/programs.

[4] European harmonized standards. [Online]. http://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/

[5] Global Certification Forum webpage. http://www.globalcertificationforum.org.

[6] PTCRB webpage https://www.ptcrb.com/index.cfm

[7] AllSeen Alliance webpage https://allseenalliance.org/

[8] AllSeen Alliance Certification Program (AllJoyn Certified) https://certify.alljoyn.org.

[9] D3.1 Progress report on the testing framework Release 1.

[10] NAPRD.03 v5.32 https://ptcrb.com/File/documents.cfm?tab=documents&ID=3 (login required)

[11] PTCRB Program Management Document (PPMD) v2.28 https://ptcrb.com/File/documents.cfm?tab=documents&ID=3 (login required).

[12] ISC License by Open Source Initiative, https://opensource.org/licenses/ISC.

[13] AllJoyn Core Interface definition: https://allseenalliance.org/framework/documentation/learn/core/about-announcement/interface

[14] AllJoyn Onboarding Interface definition: https://allseenalliance.org/framework/documentation/learn/base-services/onboarding/interface

[15] AllJoyn Notification Interface definition: https://allseenalliance.org/framework/documentation/learn/base-services/notification/interface

[16] AllJoyn Control Panel Interface definition: https://allseenalliance.org/framework/documentation/learn/base-services/controlpanel

[17] AllJoyn Gateway Interface definition: https://wiki.alljoyn.org/_media/gatewayagent/alljoyn_gateway_service_framework_interface_definition_14.12a.docx

[18] AllJoyn Test Specifications: https://certify.alljoyn.org/docs/alljoyn-certified-test-specifications

[19] Gartner Report: Worldwide Sales of Smartphones Grew 7 Percent in the Fourth Quarter of 2016: http://www.gartner.com/newsroom/id/3609817.

[20] Google Play User Interface Guidelines: https://developer.android.com/guide/practices/ui_guidelines/index.html.

[21] Microsoft App certification process: https://docs.microsoft.com/en-us/windows/uwp/publish/the-app-certification-process.

[22] Aqua Performance Testing Criteria: http://www.appqualityalliance.org/AQuA-performance-test-criteria

[23] AT&T Application Resource Optimizer (ARO):https://developer.att.com/application-resource-optimizer.

[24] The Mobile Ecosystem Forum (MEC) Privacy Policy generation tool: https://www.freeprivacypolicy.com/free-privacy-policy-generator.php).

[25] Java Verified: www.javaverified.com.

[26] Symbian Signed: http://www.symbiansigned.com (discontinued link).

[27] Microsoft Mobile2Market: http://www.microsoft.com/mobile/getcertified (discontinued link).

[28] Apple App Store App Review: https://developer.apple.com/app-store/review

[29] Google Play Store App Guidelines: https://developer.android.com/guide/practices/ui_guidelines/index.html.

[30] Windows App Certification: https://developer.microsoft.com/en-us/windows/apps/develop

[31] Privacy Policy generation tool: https://www.freeprivacypolicy.com/free-privacy-policy-generator.php.

5 Annex A: TRIANGLE Mark Certification Application Form

PRODUCT INFORMATION:

Type of product	App/ Mobile device / IoT device
Product Name	
Software Version	
Description of the product	
Additional product info (url, etc)	
Supported Use Cases	

DEVICE ADDITIONAL INFORMATION:

Model Name	
Hardware Version	

COMPANY INFORMATION

OEM name	
Address	
City	
Postal Code	
State/Providence	
Country	

CONTACT INFORMATION

Name	
email	
Phone number	

SUPPORTED USE CASES

USE CASE	Support
Virtual Reality	Yes / No
Gaming	Yes / No
Augmented Reality	Yes / No
Content Distribution Streaming Services	Yes / No
Live Streaming Services	Yes / No
Social Networking	Yes / No
High Speed Internet	Yes / No
Patient Monitoring	Yes / No
Emergency Services	Yes / No
Smart Metering	Yes / No
Smart Grids	Yes / No
Connected Vehicles	Yes / No

6 Annex B: Scenarios and use cases

Table 19 indicates the scenarios to be tested according to the use cases supported by the SUT.

Table 19 –Scenarios by use case

Network Scenarios		**Use cases**											
SC	**Scenario**	**CS**	**LS**	**SN**	**HS**	**VR**	**AR**	**GA**	**PM**	**ES**	**SM**	**SG**	**CV**
UR-OF	Urban-Office	Y		Y	Y	Y	Y	Y		Y	Y		
UR-PE	Urban-Pedestrian	Y	Y	Y	Y		Y	Y					
UR-DN	Urban-Driving-Normal	Y	Y	Y	Y		Y	Y	Y				Y
UR-DT	Urban-Driving-Traffic jam	Y		Y	Y		Y	Y	Y				Y
UR-DE	Urban-Driving-Emergency driving		Y	Y	Y		Y		Y	Y			Y
UR-IB	Urban-Internet Café, Busy Hours	Y		Y	Y	Y	Y	Y					
UR-IO	Urban-Internet Cafe, Off-Peak	Y		Y	Y	Y	Y	Y					
SU-FE	Suburban-Festival	Y	Y	Y	Y		Y	Y		Y			
SU-ST	Suburban-Stadium	Y	Y	Y	Y		Y	Y		Y			
SU-SB	Suburban-Shopping Mall, Busy Hours	Y		Y	Y		Y	Y		Y			
SU-SO	Suburban-Shopping Mall, Off-Peak	Y		Y	Y		Y	Y		Y			
HS-RE	High Speed-Relay	Y		Y	Y			Y					Y
HS-DP	High Speed-Direct Passenger Connection	Y		Y	Y			Y					Y
IT-WA	Internet of Things-Warehouse										Y		
IT-OS	Internet of Things-Outdoor Sensors										Y	Y	
IT-HS	Internet of Things-Home Sensors								Y		Y	Y	

7 Annex C: Reference Apps

Table 20 indicates the Reference Apps to be used for TRIANGLE certification testing:

Table 20 –Reference Apps

Use Case	**Reference App**
Virtual Reality	TBD
Gaming	TBD
Augmented Reality	TBD
Content Distribution Streaming Services	YouTube
Live Streaming Services	Periscope
Social Networking	Facebook
High Speed Internet	File Transfer (Android /iOS)
Patient Monitoring	TBD
Emergency Services	TBD

8 Annex D: Application User Flows

An Application User Flow is a specific list of actions that a user performs on an AUT. Application User Flows are executed to allow a Test System perform specific measurements.

Table 21 contains a list of the common Application User Flows to be used in the Test Specifications. Additional Application User Flows may be defined in each Test Specification.

Table 21 –Application User Flows

Identifier	Use Case	Application User Flow
1.1	All	Reopen the App 1. Open the App. 2. Perform login step and wait for 5 seconds. 3. Close App and wait for 5 seconds 4. Open the App (no login required).
1.2	All	Navigate menu 1. Open the App. 2. Perform login step and wait for 5 seconds. 3. Enter all available menu options and views. 4. Close the App.
1.3	All	Login 1. Perform login step and wait for 5 seconds.
2.1	CS	Play three reference videos: 1. Perform login step and wait for 10 seconds. 2. Play sequentially the three reference videos: RV1, RV2 and RV3.
2.2	CS	Play and pause 1. Perform login step and wait for 10 seconds. 2. Start playing RV3 during 10 seconds. 3. Pause the reproduction. 4. Resume the reproduction after 2 minutes
2.3	CS	Rewind and Fast Forward 1. Perform login step and wait for 10 seconds. 2. Start playing RV3 for 10 seconds. 3. Perform fast forward during 2 minutes (select X8 speed if supported by the App (ICSA_CSFastForwardX8), else select the highest speed supported). 4. Change to normal play and keep this mode for 10 seconds.

		5. Perform rewind for 2 minutes (select X8 speed if supported by the App (ICSA_CSRewindX8), else select the highest rewind speed supported), 6. Stop the playback.
2.4	CS	Download a media file 1. Perform login step and wait for 10 seconds. 2. Download RV3. 3. Wait until the download is complete.
2.5	CS	Set background state. 1. Perform login step and wait for 10 seconds. 2. Set the App in background state. 3. Wait for 20 minutes 4. Set the App in active state
2.6	CS	Play and Stop 1. Perform login step and wait for 10 seconds. 2. Start playing RV3. 3. Stop the reproduction after 1 minute. 4. Resume the reproduction after 1 minutes
2.7	CS	Search and Seek 1. Perform login step and wait for 10 seconds. 2. Search reference file RV3. 3. Start playing RV3. 4. Seek the player at 15 minutes position.
2.8	CS	Skip forward and backward 1. Perform login step and wait for 10 seconds. 2. Start playing RV2. 3. After 1 minute, skip backward to the beginning of the media file. 4. After 20 seconds, skip forward to the next media file (RV3). 5. After 5 seconds, skip backward to the previous media file (RV2).
3.1	LS	Play an live video from a know user 1. Perform login step and wait for 10 seconds. 2. Select to play the live video set up in the test case initial conditions.
3.2	LS	Broadcast live video 1. Perform login step and wait for 10 seconds. 2. Broadcast live video

4.1	SN	Post comments 1. Perform login step and wait for 10 seconds. 2. Post reference comment: RC1. 3. Post reference comment: RC2. 4. Post reference comment: RC3.
4.2	SN	Post pictures 1. Perform login step and wait for 10 seconds. 2. Post sequentially the pictures: RP1, RP2 and RP3 and without any delay between the pictures. 3. Wait until the last picture is completely uploaded.
4.3	SN	Post videos 1. Perform login step and wait for 10 seconds. 2. Post sequentially the pictures: RV1, RV2 and RV3 and without any delay between videos. 3. Wait until the last video is completely uploaded.
4.4	SN	Post live video 1. Perform login step and wait for 10 seconds. 2. Post sequentially the pictures: RV1, RV2 and RV3 and without any delay between videos. 3. Wait until the last video is completely uploaded.
4.5	SN	Post location 1. Perform login step and wait for 10 seconds. 2. Post sequentially the reference location: RL1.
4.6	SN	Post files 1. Perform login step and wait for 10 seconds. 2. Post sequentially the reference files: RF1, RF2 and RF3. 3. Wait until all the files are completely uploaded.
4.7	SN	Get comment 1. Perform login step and wait for 10 seconds. 2. Get the first available comment.
4.8	SN	Show picture 1. Perform login step and wait for 10 seconds. 2. Get the first available picture.
4.9	SN	Play video 1. Perform login step and wait for 10 seconds. 2. Get the first available video.
4.10	SN	Play live video

		1. Perform login step and wait for 10 seconds. 2. Get reference live video
4.11	SN	Get location 1. Perform login step and wait for 10 seconds. 2. Post sequentially the reference location: RL1.
4.12	SN	Get file 1. Perform login step and wait for 10 seconds. 2. Get the first available file.
4.13	SN	Search objects 1. Perform login step and wait for 10 seconds. 2. Search the most relevant item for which the App has been mainly designed (e.g., contacts, flights, hotels, etc.).
5.1	HS	Download three files sequentially 1. Perform login step and wait for 10 seconds. 2. Download sequentially the reference files: RF1, RF2 and RF3 and without any delay between them. 3. Wait until the last file is completely downloaded.
5.2	HS	Upload three files sequentially 1. Perform login step and wait for 10 seconds. 2. Upload sequentially the reference files: RF1, RF2 and RF3 and without any delay between them. 3. Wait until the last file is completely uploaded.
5.3	HS	Download several files simultaneously 1. Perform login step and wait for 10 seconds. 2. Download simultaneously the reference files: RF1, RF2, RF3, RF4, RF5 and RF6. 3. Wait until the last file is completely downloaded.
5.4	HS	Upload several files sequentially 1. Perform login step and wait for 10 seconds. 2. Upload simultaneously the reference files: RF1, RF2, RF3, RF4, RF5 and RF6. 3. Wait until the last file is completely uploaded.
5.5	HS	Download a huge file 1. Perform login step and wait for 5 seconds. 2. Download the reference file RF7. 3. Wait until the file is completely downloaded.
5.6	HS	Upload a huge file

		1. Perform login step and wait for 5 seconds. 2. Upload the reference file RF7. 3. Wait until the last file is completely uploaded.
5.7	HS	Pause and Resume Download 1. Perform login step and wait for 10 seconds. 2. Start downloading the reference file RF7. 3. After 30 seconds, pause the file transfer. 4. Wait for 15 seconds and resume the transfer
5.8	HS	Pause and Resume Upload 1. Perform login step and wait for 10 seconds. 2. Start uploading the reference file RF7. 3. After 30 seconds, pause the file transfer. 4. Wait for 15 seconds and resume the file upload.
6.1	VR	Load Virtual Experience 1. Perform login step and wait for 10 seconds. 2. Load reference virtual experience RVE1. 3. Load until the virtual experience is completely loaded
7.1	AR	Load Augmentation layer on physical marker 1. Perform login step and wait for 10 seconds. 2. Start an augmented reality session. 3. Aim at a physical marker.
7.2	AR	Load Augmentation layer at a location 1. Perform login step and wait for 10 seconds. 2. Start an augmented reality session. 3. Aim at a specific location.
8.x	PM	TBD
9.x	ES	TBD
10.1	GA	Start session game 1. Perform login step and wait for 10 seconds. 2. Set most common configuration (as required) 3. Start session game
10.2	GA	Short Session game 1. Perform login step and wait for 10 seconds. 2. Set game most common configuration. 3. Start game.

		4. Perform standard game session for 2 minutes
10.3	GA	Large Session game 1. Perform login step and wait for 10 seconds. 2. Set game most common configuration. 3. Start game. 4. Perform standard game session for 15 minutes
10.4	GA	Pause and resume game 1. Perform login step and wait for 5 seconds. 2. Set game most common configuration. 3. Start game session. 4. After 2 minutes set the session in pause mode. 5. After 30 seconds resume the game session.
10.5	GA	Start saved session game 1. Perform login step and wait for 5 seconds. 2. Set game most common configuration. 3. Start game session. 4. After 2 minutes save game session data. Note: Some Apps may need a longer time to allow saving game session. 5. Exit the game session. 6. After 10 seconds restart the saved game session. 7. After 20 seconds, exit the game session.
10.6	GA	Start two game sessions 1. Perform login step and wait for 10 seconds. 2. Set most common configuration (as required). 3. Start a new session game. 4. After 1 minute, exit the game session. 5. Exit the game session and wait for 15 seconds. 6. Start a new session game. 7. After 15 seconds, exit the game session.

Where:

- RV1: Reference video 1 (Short duration video): TBD
- RV2: Reference video 2 (Medium duration video): TBD
- RV3: Reference video 3 (Long duration video (at least 30 minutes)): TBD

- RP1: Reference picture 1 (Small size picture): TBD
- RP2: Reference picture 2 (Medium size picture): TBD
- RP3: Reference picture 3 (Large size picture): TBD
- RC1: Reference comment 1: “The rain in Spain stays mainly in the plain.”
- RL1: Reference location 1: TBD
- RF1: Reference file 1 (Small size file): TBD
- RF2: Reference file 2 (Medium size file): TBD
- RF3: Reference file 3 (Large size file): TBD
- RF4: Reference file 4 (Large size file): TBD
- RF5: Reference file 5 (Large size file): TBD
- RF6: Reference file 6 (Large size file): TBD
- RVE1: Reference Virtual Experience 1: TBD
- RTVP1: Reference Fixed TV Pattern 1: TBD
- RTVP2: Reference TV Pattern 2 (High definition): TBD

Note: Items with ‘TBD’ will be defined once the project obtains more experience testing.

9 Annex E: An example of product certification: BlueEye IoT device

9.1 Introduction

The BlueEye wearable system is an alpha customer of the TRIANGLE testbed for IoT devices as indicated in section 12 of [9].

This Annex initially presents the main function and applications of the BlueEye, highlighting the aspects more relevant for the TRIANGLE Testing Framework.

This Annex also describes the certification process to be carried for the BlueEye product and the relevant information handled during the process, from ICS/IXIT data and definition of the Test Plan to the performance of test cases and obtaining product KPIs and scoring.

9.2 BlueEye IoT device

BlueEye is a wearable video system based on a glass-mounted camera including audio, which enables live interactive point of view video to be streamed to a command center, hospital emergency department or hot desk to provide real time interactive support.

BlueEye is a LTE device whose main functionality is the transmission of simple video and duplex audio in real time.

BlueEye, by means of LTE or Wi-Fi connectivity is able to transmit, in real time, image captured by the video camera, to an Backend application running in a Host, from where it is possible to configure and to establish different classes of services.

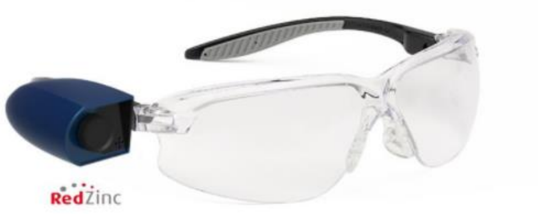


Figure 8 – BlueEye IoT device

Figure 9 – BlueEye application

BlueEye improves patient outcome in pre-hospital emergencies by helping provide oversight, diagnosis and treatment via wireless video link.

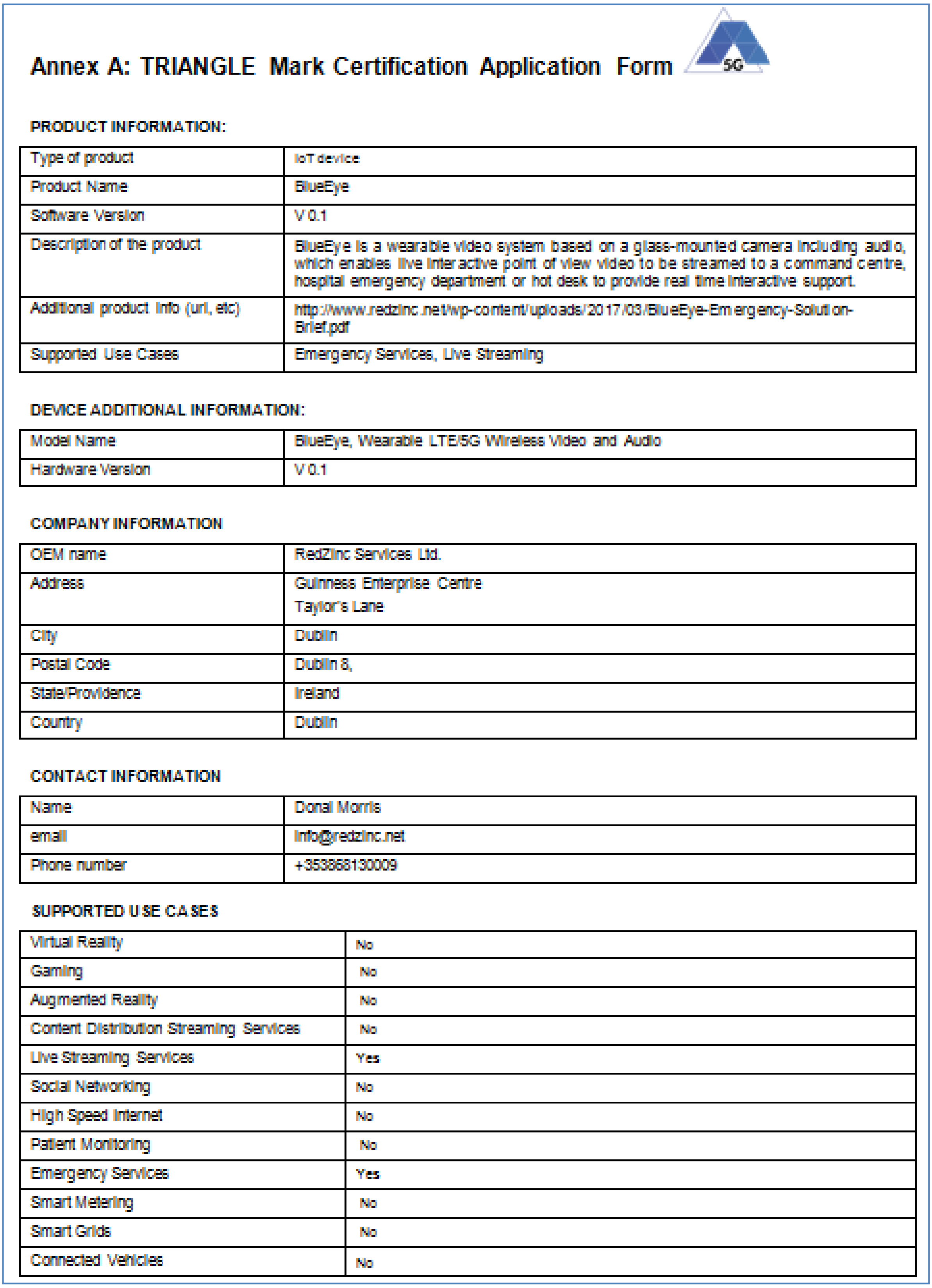
9.3 BlueEye and TRIANGLE Mark

This section describes the relevant steps to be performed during the TRIANGLE certification of BlueEye product and the information provided and obtained during those steps.

9.3.1 Certification Application

Once the manufacturer of BlueEye product (Redzinc) decides to certify its product, firstly it will fill and send a Certification Application Form to TRIANGLE.

Figure 10 shows an example of BlueEye Certification Application.



Annex A: TRIANGLE Mark Certification Application Form

PRODUCT INFORMATION:

Type of product	IoT device
Product Name	BlueEye
Software Version	V 0.1
Description of the product	BlueEye is a wearable video system based on a glass-mounted camera including audio, which enables live interactive point of view video to be streamed to a command centre, hospital emergency department or hot desk to provide real time interactive support.
Additional product info (url, etc)	http://www.redzinc.net/wp-content/uploads/2017/03/BlueEye-Emergency-Solution-Brief.pdf
Supported Use Cases	Emergency Services, Live Streaming

DEVICE ADDITIONAL INFORMATION:

Model Name	BlueEye, Wearable LTE/5G Wireless Video and Audio
Hardware Version	V 0.1

COMPANY INFORMATION

OEM name	RedZinc Services Ltd.
Address	Guinness Enterprise Centre Taylor's Lane
City	Dublin
Postal Code	Dublin 8,
State/Providence	Ireland
Country	Dublin

CONTACT INFORMATION

Name	Donal Morris
email	info@redzinc.net
Phone number	+353868130009

SUPPORTED USE CASES

Virtual Reality	No
Gaming	No
Augmented Reality	No
Content Distribution Streaming Services	No
Live Streaming Services	Yes
Social Networking	No
High Speed Internet	No
Patient Monitoring	No
Emergency Services	Yes
Smart Metering	No
Smart Grids	No
Connected Vehicles	No

Figure 10 – BlueEye Certification Application

9.3.2 ICS/IXIT

Redzinc needs to provide ICS/IXIT proforma to TRIANGLE, declaring the main functionalities of its product and other data required to perform the testing.

An example of filled ICS/IXIT proforma for BlueEye product is shown in Figures 11 and 12.

ICS/IXIT tables are obtained from Appendix 2 delivered together with this document.

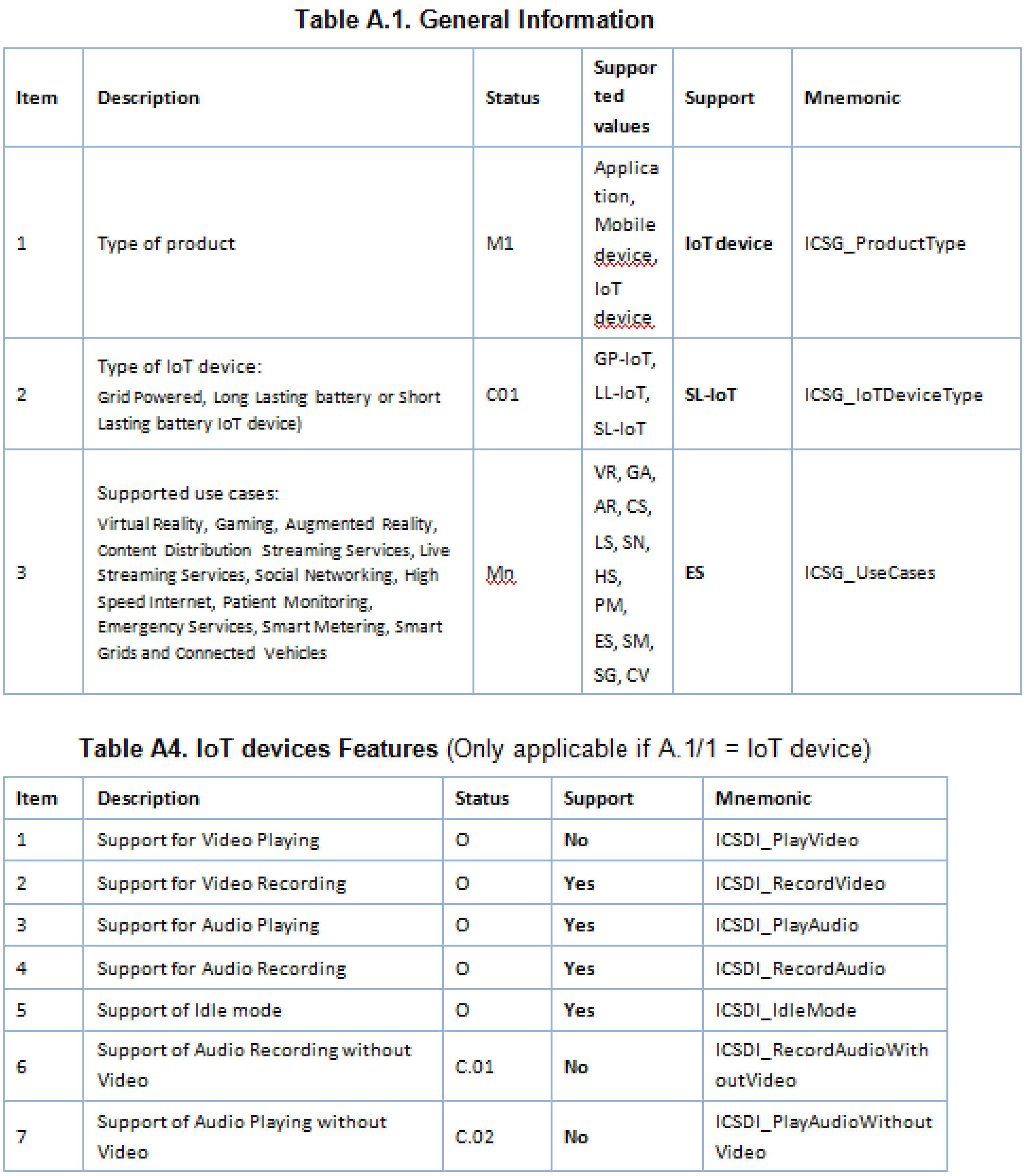


Table A.1. General Information

Item	Description	Status	Supported values	Support	Mnemonic
1	Type of product	M1	Application, Mobile device, IoT device	IoT device	ICSG_ProductType
2	Type of IoT device: Grid Powered, Long Lasting battery or Short Lasting battery IoT device)	C01	GP-IoT, LL-IoT, SL-IoT	SL-IoT	ICSG_IoTDeviceType
3	Supported use cases: Virtual Reality, Gaming, Augmented Reality, Content Distribution Streaming Services, Live Streaming Services, Social Networking, High Speed Internet, Patient Monitoring, Emergency Services, Smart Metering, Smart Grids and Connected Vehicles	Mn	VR, GA, AR, CS, LS, SN, HS, PM, ES, SM, SG, CV	ES	ICSG_UseCases

Table A4. IoT devices Features (Only applicable if A.1/1 = IoT device)

Item	Description	Status	Support	Mnemonic
1	Support for Video Playing	O	No	ICSDI_PlayVideo
2	Support for Video Recording	O	Yes	ICSDI_RecordVideo
3	Support for Audio Playing	O	Yes	ICSDI_PlayAudio
4	Support for Audio Recording	O	Yes	ICSDI_RecordAudio
5	Support of Idle mode	O	Yes	ICSDI_IdleMode
6	Support of Audio Recording without Video	C.01	No	ICSDI_RecordAudioWithoutVideo
7	Support of Audio Playing without Video	C.02	No	ICSDI_PlayAudioWithout Video

Figure 11 – BlueEye ICS

Note: Appendix 2 Table A.2 only applies to Applications and Appendix 2 Table A.3 only applies to mobile devices.

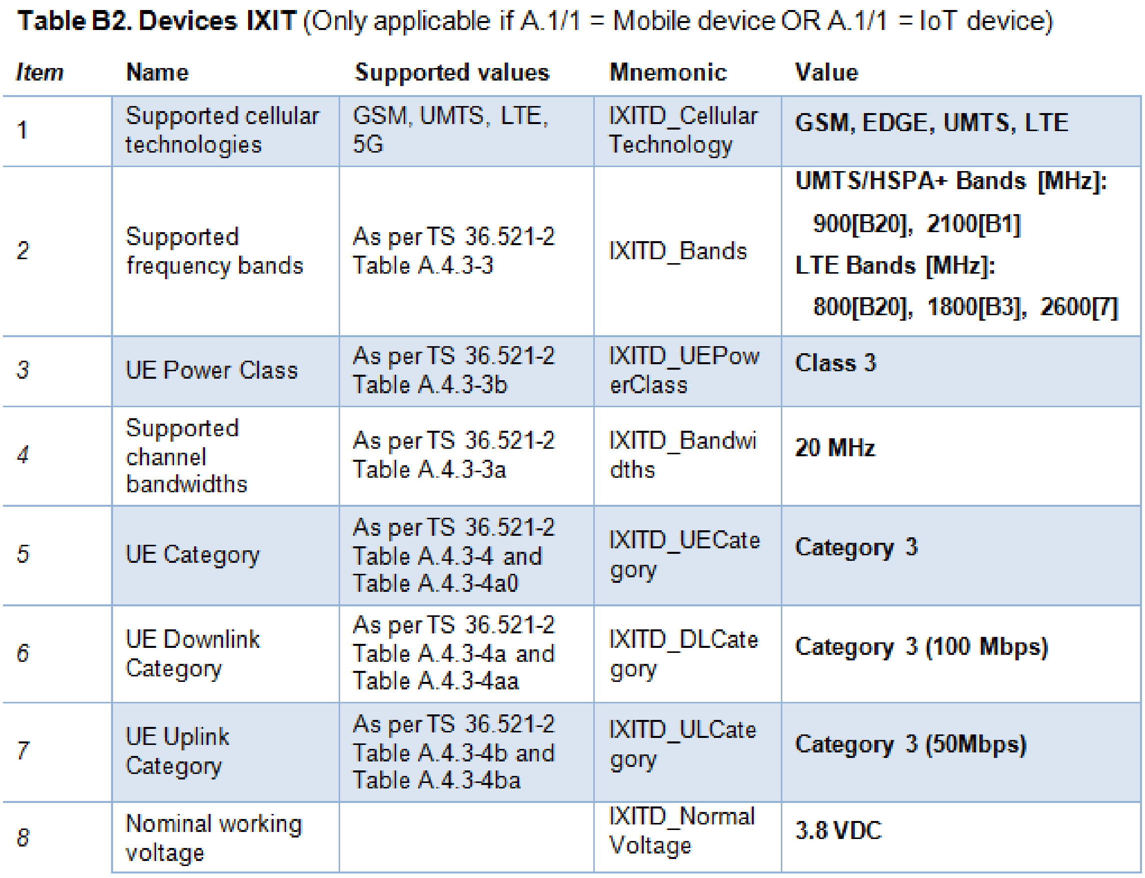


Table B2. Devices IXIT (Only applicable if A.1/1 = Mobile device OR A.1/1 = IoT device)

Item	**Name**	**Supported values**	**Mnemonic**	**Value**
1	Supported cellular technologies	GSM, UMTS, LTE, 5G	IXITD_Cellular Technology	**GSM, EDGE, UMTS, LTE**
2	Supported frequency bands	As per TS 36.521-2 Table A.4.3-3	IXITD_Bands	**UMTS/HSPA+ Bands [MHz]:** **900[B20], 2100[B1]** **LTE Bands [MHz]:** **800[B20], 1800[B3], 2600[7]**
3	UE Power Class	As per TS 36.521-2 Table A.4.3-3b	IXITD_UEPowerClass	**Class 3**
4	Supported channel bandwidths	As per TS 36.521-2 Table A.4.3-3a	IXITD_Bandwidths	**20 MHz**
5	UE Category	As per TS 36.521-2 Table A.4.3-4 and Table A.4.3-4a0	IXITD_UECategory	**Category 3**
6	UE Downlink Category	As per TS 36.521-2 Table A.4.3-4a and Table A.4.3-4aa	IXITD_DLCategory	**Category 3 (100 Mbps)**
7	UE Uplink Category	As per TS 36.521-2 Table A.4.3-4b and Table A.4.3-4ba	IXITD_ULCategory	**Category 3 (50Mbps)**
8	Nominal working voltage		IXITD_Normal Voltage	**3.8 VDC**

Figure 12 – BlueEye IXIT

9.3.3 TRIANGLE domains

Being an IoT Device, the domains applicable to BlueEye are the ones shown in the Table 22:

Table 22 –BlueEye applicable TRIANGLE domains

System under Test	**Domain**	**Identifier**	**Test Specification**
IoT device	Reliability	IDR	IoT Devices Reliability
IoT device	Network Adaptation	INA	IoT Devices Network Adaptation
IoT device	Radio Performance	IRP	IoT Devices Radio Performance
IoT device	Data Performance	IDP	IoT Devices Data Performance
IoT device	Energy Consumption	IEC	IoT Devices Energy Consumption

9.3.4 Test Plan

TRIANGLE will generate the Test Plan (list of test cases to be executed on BlueEye IoT device to evaluate its performance).

The Test Plan is obtained getting data form Redzinc ICS/IXIT proforma (defined in Appendix 2) and based on the list of test cases included in TRIANGLE TCRL (defined in Appendix 3).

Table 22 lists the test cases composing the Test Plan for BlueEye product based on TRIANGLE TCRL (As stated in Appendix 3 of this document), Redzinc ICS/IXIT proforma (section 9.3.2) and the test cases applicability tables specified in each Test Specification.

Table 23 –BlueEye Certification Test Plan

Test case Id	**Description**
IEC/CO/001	Energy Consumption. IUT in idle mode
IEC/ES/001	Energy Consumption Send video streaming
IEC/ES/003	Energy Consumption Receive video streaming
IDP/ES/001	Data Performance. IUT in idle mode
IDP/ES/002	Data Performance. Send video streaming
IDP/ES/003	Data Performance. Receive video streaming

IDR/ES/001	Reliability. Send video streaming
IDR/ES/003	Reliability. Receive video streaming
IDR/ES/005	Reliability. Power failure when sending video streaming
IDR/ES/007	Reliability. Power failure when receiving video streaming

Note: Additional test cases shall be added to the certification test plan when new Test Specifications are released.

On the other hand, each test case will be executed on all the scenarios applicable for BlueEye supported use cases. As BlueEye supports 'Emergency Services' use case, and according to Annex B of this document, the applicable scenarios shall be:

Table 24 –BlueEye testing scenarios

SC	**Scenario**	**Emergency Services**
UR-OF	Urban-Office	Y
UR-DE	Urban-Driving-Emergency driving	Y
SU-FE	Suburban-Festival	Y
SU-ST	Suburban-Stadium	Y
SU-SB	Suburban-Shopping Mall, Busy Hours	Y
SU-SO	Suburban-Shopping Mall, Off-Peak	Y

9.3.5 Measurements

Based on the Test Plan defined in previous section, the measurements defined in Table 25 will be performed during test cases execution.

Table 25 –BlueEye test cases' measurements

Test case Id	**Description**	**Measurement**
IEC/CO/001	Energy Consumption. IUT in idle mode	Current consumption
IEC/ES/001	Energy Consumption Send video streaming	Current consumption
IEC/ES/003	Energy Consumption Receive video streaming	Current consumption
IDP/ES/001	Data Performance. IUT in idle mode	PDSCH data. PDCCH data. PUSCH data. PUCCH data. UL/DL PDCPs data. UL/DL S1-U data. UL/DL S1-MME data. UL/DL S5/ePDG data.

		Number of bearers. Type of bearers. TCP/UDP connections.
IDP/ES/002	Data Performance. Send video streaming	PDSCH data. PDCCH data. PUSCH data. PUCCH data. UL/DL PDCPs data. UL/DL S1-U data. UL/DL S1-MME data. UL/DL S5/ePDG data. Number of bearers. Type of bearers. TCP/UDP connections
IDP/ES/003	Data Performance. Receive video streaming	PDSCH data. PDCCH data. PUSCH data. PUCCH data. UL/DL PDCPs data. UL/DL S1-U data. UL/DL S1-MME data. UL/DL S5/ePDG data. Number of bearers. Type of bearers. TCP/UDP connections
IDR/ES/001	Reliability. Send video streaming	Playback Availability Playback Cutoff Content Stall Frames Loss Video Resolution
IDR/ES/003	Reliability. Receive video streaming	Playback Availability Playback Cutoff Content Stall Frames Loss Video Resolution
IDR/ES/005	Reliability. Power failure when sending video streaming	Playback Availability Playback Cutoff Content Stall Frames Loss Video Resolution Recovery Time
IDR/ES/007	Reliability. Power failure when receiving video streaming	Playback Availability Playback Cutoff Content Stall Frames Loss Video Resolution Recovery Time

9.3.6 KPIs

After the Test Plan has been executed and all the measurements have been performed, BlueEye KPIs are calculated based on the measurements performed.

BlueEye related KPIs are defined in Table 26.

Table 26 –BlueEye KPIs

KPI	**Measurements**
OTA DL U-plane throughput	Current Consumption
OTA DL U-plane throughput	PDSCH data
OTA DL C-plane throughput	PDCCH data
OTA UL U-plane throughput	PUSCH data
OTA UL C-plane throughput	PUCCH data
PDCP-SAP goodput UL/DL	UL/DL PDCPs data
Number of bearers	Number of established bearers
Number of transport connections	Number of opened TCP/UDP connections
Burst inter-generation time at transport level	UL/DL S1-U data
	UL/DL S1-MME data
Availability	Playback Availability
	Playback Cutoff
Content Stall	Content Stall
Frame Loss Rate (%)	Frames Loss
Content Resolution	Video Resolution
Recovery after fail	Playback Availability after power failure
	Playback Cutoff after power failure
	Content Stall after power failure
	Frames Loss after power failure
	Video Resolution after power failure
Recovery Time	Recovery Time

Note: IoT devices Radio Performance Test Specification and IoT devices Network Adaptation have not been released yet. When those Test Specifications are releases new KPIs will be defined such Sensitivity, Adjacent channel selectivity, Maximum Output signal and Co-channel rejection for Radio Performance domain and, Video and audio quality and delay of the video/audio transmission in the case of Network adaptation domain.

9.3.7 Scoring and TRIANGLE mark

Once BlueEye KPIs are obtained, and according to the process defined in Appendix 1. Scoring (comparing BlueEye KPIs with reference values defined by TRIANGLE), BlueEye scoring is obtained. Figure 13 shows and Spider Web diagram example of results where BlueEye scoring is shown in blue color and reference value is shown in yellow color (values in the figure are not real).

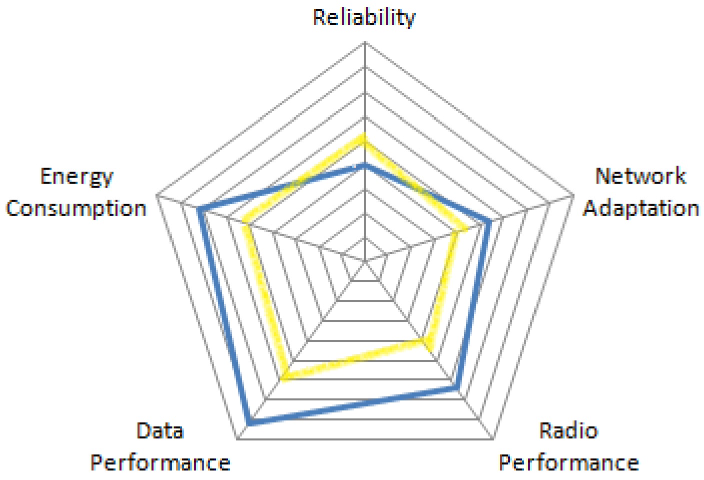


Figure 13 – Example of BlueEye spider web diagram (data not real)

Finally, when all certification requirements are met, the TRIANGLE mark will be issued.

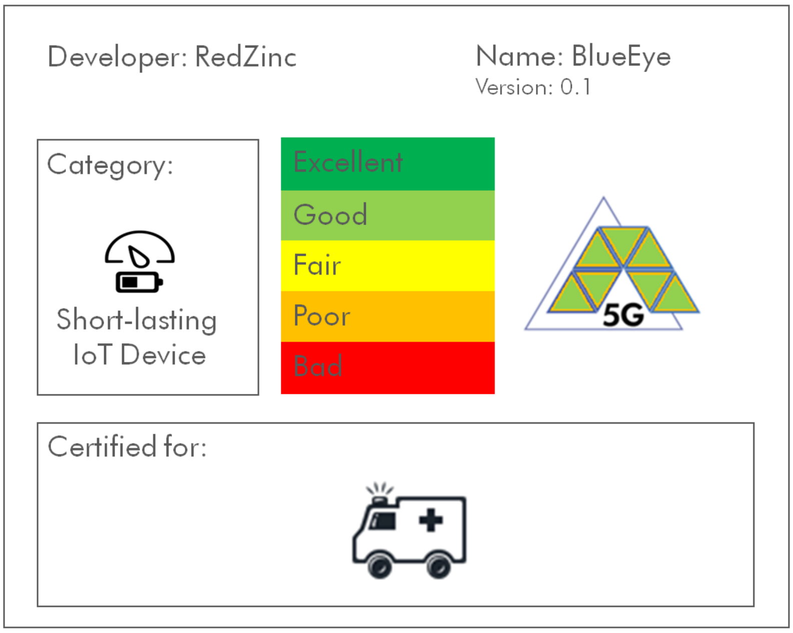


Figure 14 – Example of BlueEye TRIANGLE mark