GCF
Test Certify Connect

Introductory Guide to MCS Certification

June 2025

This guide issued by GCF and TCCA provides a high-level overview of the GCF Certification programme for various MCX product types, and is meant for procurement specialists and business professionals of organisations providing services based on 3GPP Mission Critical technology, to get a better understanding of the certification requirements for these products, and to ensure that products being procured are GCF Certified, by including the necessary requirements in contract tenders for MCX products and solutions.

www.globalcertificationforum.org

Table of Contents

1 Scope

As Mission Critical Communications Operators (MCCO) globally undertake the migration of their Public Land Mobile Radio networks from narrowband (TETRA/P25) to Mobile Broadband based systems (3GPP MCX), certification of Mission Critical products and solutions becomes all the more important to ensure both compliance to industry standards and interoperability with other 3GPP compliant Mission Critical systems.

This document provides a high-level overview of the GCF Certification programme for various MCX product types, and is meant for procurement specialists and business professionals of organisations providing services based on 3GPP Mission Critical technology, to get a better understanding of the certification requirements for these products, and to ensure that products being procured are GCF Certified, by including the necessary requirements in contract tenders for MCX products and solutions.

2 Abbreviations & Definitions

3GPP	3rd Generation Partnership Project is a Standards Development Organisation that develops and maintains standards for the Telecommunications and Mission Critical Broadband ecosystems
ACE	Assessment Capable Entity are subject matter experts on GCF Certification from member companies, who facilitate the Manufacturer through the certification process. A list of ACEs is available on the GCF member portal.
GCF	Global Certification Forum, an industry organisation that develops and maintains certification programmes for wirelessly connected products typically based on the 3GPP standards
GSMA	The GSM Association, an industry organisation that develops and maintains requirements and standards for wireless products and solutions and that are complementary to 3GPP specifications
IP	Internet Protocol used for communicating between wired or wirelessly connected systems
LRWG	Legal and Regulatory Working Group, a working group under the TCCA for Public Safety Operator members of TCCA who examine, provide guidance on and identify lacunae of legislation & regulation impacting critical comms.
MCX	Mission Critical Services comprised of MCPTT, MCVideo, and MCData, where X denotes any one or all of the aforementioned services
MCCO	Mission Critical Communications Operators also referred to as Public Safety Agencies, and/or any operator of a Mission Critical Network
MCPTT	Mission Critical Push to Talk services
MCVideo	Mission Critical Video services
MCData	Mission Critical Data services
MCSWS	Mission Critical Services Work Stream, a working group established by the GCF and TCCA to develop and manage the MCX Certification Programme
QPP	Quality, Priority and Pre-emption typically used by Mission Critical service providers to ensure the appropriate Quality of Service, Prioritisation of calls for emergency professionals over other users, and in some cases securing the communication channel for the exclusive use of emergency services (pre-emption)
RTO	Recognised Test Organisations are test laboratories who are accredited to perform certification testing. A list of RTOs and their areas of testing are available on the GCF Member's Portal.
SDK	Software Development Kit, often used by product suppliers to develop their final products for commercialisation.
SDO	Standards Development Organisation such as the 3GPP
TCCA	The Critical Communications Association, an industry organisation that globally advocates for the adoption of standards based MCX technology for the Mission Critical Industry
UE	User Equipment, typically a hand-held device, such as a smartphone that is GCF certified to 3GPP standards

3 Mission Critical Broadband Ecosystem

The Mission Critical Broadband ecosystem comprises of a UE with an integrated or downloaded MCX Client communicating with a MCX Server over a 4G or 5G cellular broadband network, as well as other MCX UEs via 5G Proximity Services (i.e. Sidelink, when available).

The MCX Server may be connected to other MCX Servers as part of a larger public safety network, and/or to servers that belong to other public safety agencies as part of an interoperable system, as well as to a dispatcher client located in the centralised Control Room. MCX Broadband networks may also have connectivity to legacy TETRA/P.25 communication systems via the Interworking (IWF) function.

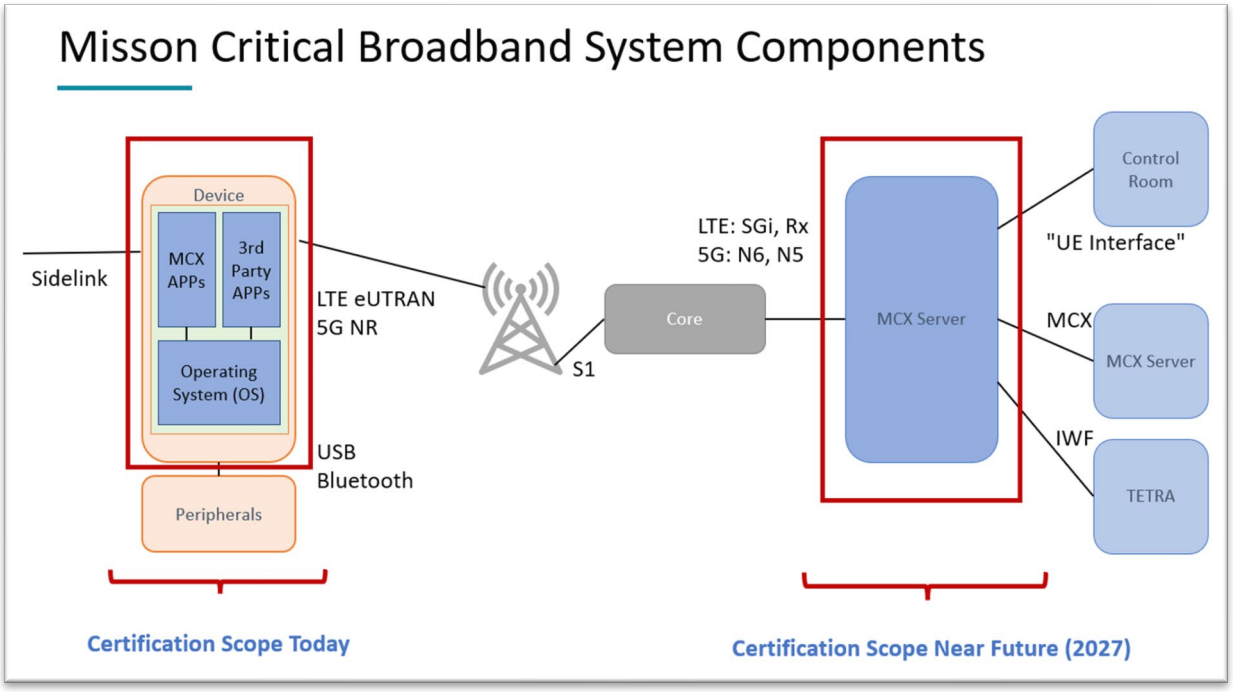

Figure 1: Mission Critical Broadband System

While the MCX communication takes place over an IP connection between the client and server, and can technically be executed over any wireless/wired connection, certain critical features such as Quality of Service, Priority, and Pre-emption (QPP) specific to cellular networks, require integration and support of the MCX systems with the underlying 4G and/or 5G network elements. As such, the certification of MCX products not only check the MCX specific features and functionality that run over IP, but also those features and functionality that are required to be supported by the radio access technology.

3.1 MCX Product Types

Currently the following Product Types are being supported in GCF Certification:

- **MCX SW Clients** & Platforms (integrated or downloaded on a UE that enables MCX over Cellular Broadband). A Client is considered a fully functional MCX application that is commercially available for purchase and use by the MCCO. A Client Platform is a fully functional MCX application that is available only to other product suppliers for integration into an end product. As an example, the MCX Client SDK can be certified as a Client Platform, which a product supplier then uses to develop their own Client for commercialisation.

- **MCX UE** (4G and/or 5G GCF Certified devices that have appropriate enablers such as QCI/5QI, dedicated bearers, UE AMBR, PDP/PER, PPDR Bands etc., supported for MCX operation).

  NOTE: Not all GCF Certified UEs can be considered MCX UEs, as they may only support general 3GPP standards and may not have support for MCX specific enablers, such as the appropriate QCI support. It is up to the MCCO to ensure that all UEs being procured support MCX services as defined in the GCF Certification Criteria.

The following product types are on the GCF Certification roadmap and will be supported once all standardization dependencies have been met (2027+):

- **MCX Dispatcher** (Clients installed in a Control Room over Fixed IP access)
- **MCX Servers** (Backend servers that communicate with MCX clients or other MCX servers)
- **MCX IWF** (Interworking Function to allow communication of MCX over Broadband with TETRA, P.25, etc.)
- **MCX IoT Telematics Blade** (a translation entity comprised of MCX Client with associated business logic, that sits on the network edge and that provides message translation services between MCX systems and IoT Telematics systems

While the ultimate goal for the GCF MCX Certification Programme is to have the entire system of products and solutions certified, different product types are being introduced in phases once external dependencies, such as standardisation requirements from 3GPP are met, as such, MCCO's are encouraged to demand certified products and solutions based on certification of product types that are available in the GCF MCX Certification Programme at the time of product procurement.

4 Mission Critical Services Product Certification

4.1 GCF Wireless Product Certification

The Global Certification Forum (GCF) Ltd., develops, maintains and manages a certification scheme for wireless products that are based on technology that is standardised by SDOs such as the 3GPP. In order to certify their product, a product supplier must first become a GCF Manufacturer Member in either the Full, Associate Manufacturer Member I (AMM I) or Associate Manufacturer Member II (AMM II) membership category.

The Certification Criteria for Mission Critical Services are captured in a dedicated Permanent Reference Document, the GCF-MCS PRD, which all suppliers undertaking certification must review, and is available for download from both the MCSWS and GCF Member's Portal.

Certification is comprised of:

- **Conformance Testing** – This is testing that is conducted on the product in an ISO 17025 accredited laboratory against test equipment that simulates the wireless service (Radio Access Network and various Application Servers). The purpose of Conformance Testing is to ensure product compliancy to the standard. Conformance Testing is a **Mandatory** requirement for GCF MCX Certification.

- **Interoperability Testing** – This is testing that is conducted on the product in a controlled lab environment against a test bed using real network elements and servers that are configured to offer the service. The purpose of Interoperability Testing is to ensure that the product under test interoperates correctly with other compliant products, systems and solutions. Interoperability Testing will become **Mandatory**, unless Field Trials is also conducted, once the programme is activated in early 2026.

- **Field Trials Testing** – This is testing that is conducted on the product in a commercial network where the service is available. The purpose of Field Trials Testing is to ensure the product under test interoperates with networks that have been commercially deployed across the world. Given the sensitive nature of Mission Critical Communications networks, access may be restricted, hence MCX Field Trials is **Optional** in GCF, and must be requested and access to the test lab approved by the MCCO on their networks. MCS Field Trials testing will be activated in GCF Certification when a MCCO makes their network available for testing as part of a Field Trial Qualified Network offering.

  NOTE: For UEs to be used in consumer or mission critical, Field Trials Testing as part of the standard GCF Certification (non-MCX areas) will be required as defined in the GCF Certification Criteria.

- **Performance Testing** – This is testing that is conducted in a lab and checks how well the product is performing under the service offering. Performance tests do not have a pass/fail criterion but typically reports back metrics that allows the MCCO to evaluate a product against a benchmark or average set of metrics from other certified products. Performance Testing is **Optiona**l in GCF, and would have to be requested by the MCCO from their product suppliers, should they want it conducted.

It is important to note that the Product Manufacturer will have to procure the services of the following GCF Certification Ecosystem actors in order to complete their certification:

- **Third Party Assessment Capable Entity (TP-ACE):** These are subject matter experts in GCF Certification from member companies, who facilitate the Manufacturer through the certification process. A list of ACEs is available on the GCF member portal:

  https://www.globalcertificationforum.org/third-party-assessment-capable-entities.html \

- **Third Party Recognised Test Organisation (RTO):** These are test laboratories who are accredited to perform certification testing in a specific technology area, such as MCS. A list of RTOs and their areas of testing are available on the GCF Member's Portal:

  https://www.globalcertificationforum.org/rto.html

  It is important to note that GCF has RTOs for Conformance Testing, Interoperability Testing and Field Trials Testing, and hence the services of different RTOs may be required to undertake a certification.

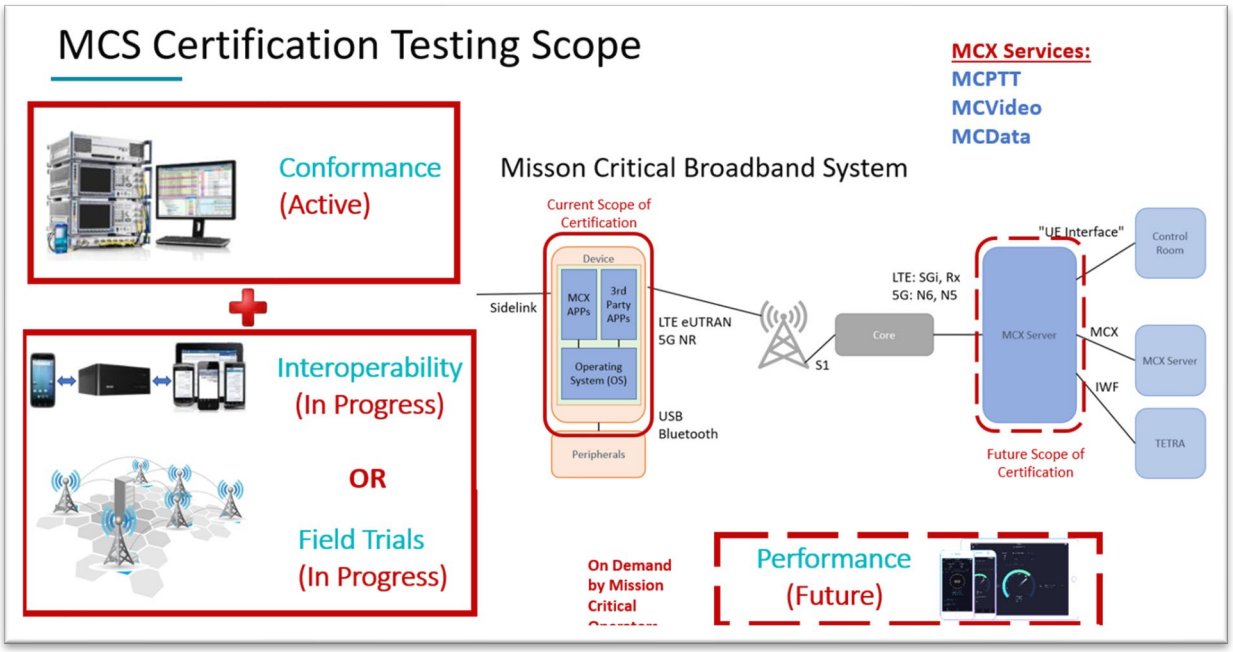

Figure 2: MCS Certification Testing Scope

The 7-Step GCF Certification Process is depicted in Figure 3 below.

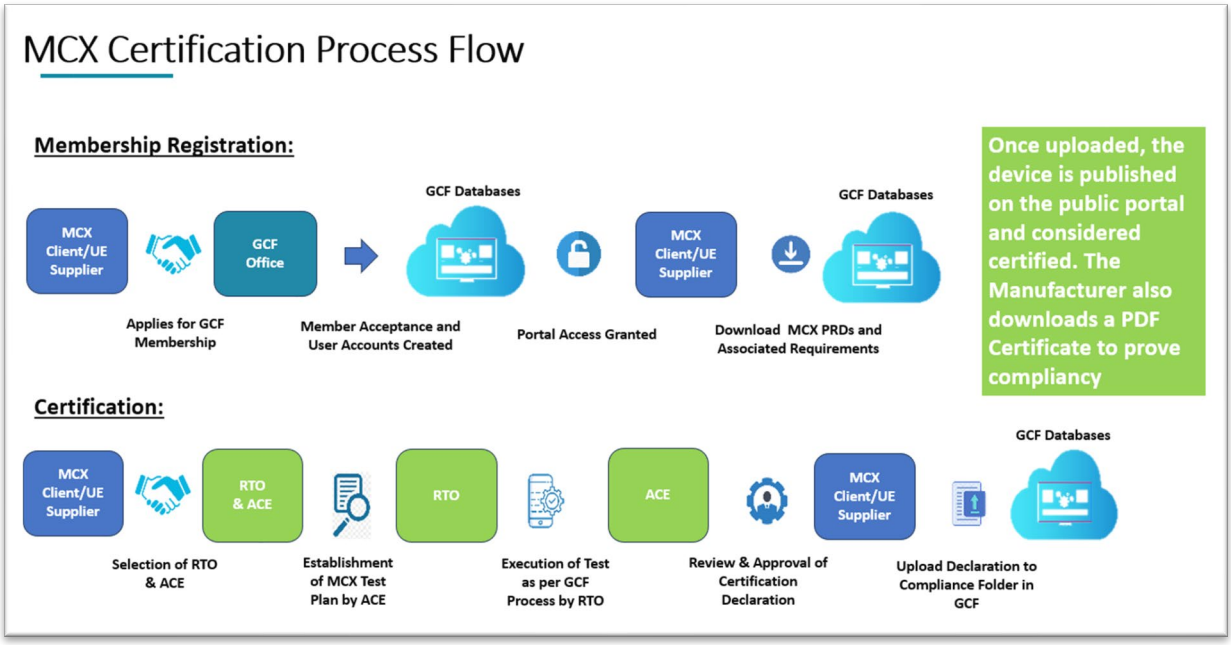

Figure 3: GCF MCX Certification Process

4.2 MCX Routes to Certification

The Mission Critical Services Workstream (MCSWS) have established four potential routes a Product Manufacturer can take to complete their certification:

1. **Native Integration of an MCX Client on an End Product (UE/Device)**
2. **Integration of a GCF Certified MCX Client Platform on an End Product (UE/Device)**
3. **Integration of an MCX Client on a GCF Certified UE/Device platform**
4. **MCX Client only Certification**

4.2.1 Route 1: Native Integration of an MCX Client on an End Product (UE/Device)

This route is available for a UE Product Manufacturer who has integrated MCX application functionality natively on the UE, and would like to certify their UE to 3GPP & GSMA standards, which includes MCX technology. This is in most respects a "standard" GCF Certification, as MCX technology is considered an additional feature of the UE. The Manufacturer would follow the process as outlined by the GCF to certify their product as per Figure 3 below. The Manufacturer at all times, throughout the lifecycle of the product, is responsible for the UE being compliant to the standards, i.e. after commercialisation if the software on the UE is updated that affects the technology area that was certified, such as introducing a new function, they would need to update their certification in GCF with the appropriate testing of the new functionality and regression testing of other areas, and upload their declarations to the GCF compliance folder.

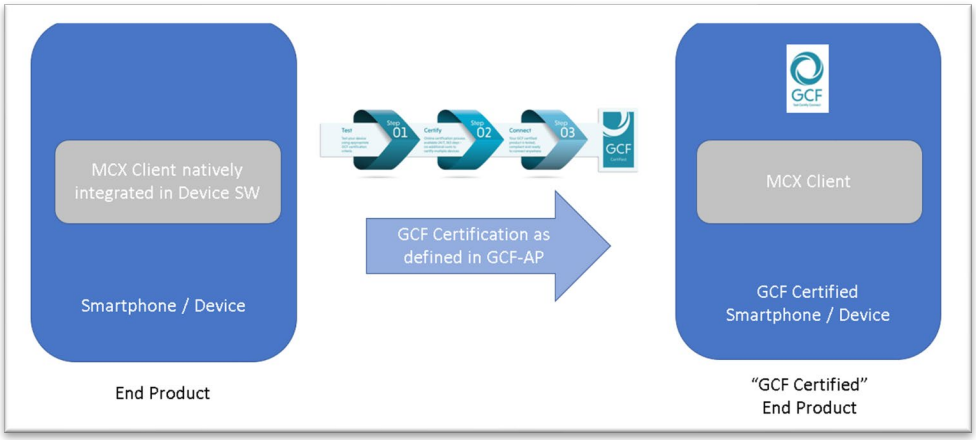

Figure 4: Route 1 – Native Integration of an MCX Client on an End Product (UE/device)

4.2.2 Route 2: Integration of a GCF Certified MCX Client Platform on an end product

This route is available for a UE Product Manufacturer that integrates a GCF Certified MCX client platform in the UE. In this case the UE supplier would have a commercial agreement with a MCX Client supplier to integrate their already certified MCX Client Platform (done via Route 4), and would undertake certification of the combined system.

The MCX Client Platform supplier would be responsible for the compliance of the Client functionality, and the UE supplier would be responsible for the integration and compliance of the end product to the standards throughout the commercial life cycle of the product.

Process for undertaking GCF Certification for Mission Critical Services utilising a GCF Certified MCX Client Platform on an end product is shown below:

Figure 5: Route 2 – Integration of a GCF Certified MCX Client Platform on an end product

4.2.3 Route 3: Integration of an MCX Client on a GCF Certified device platform

Route 3 is similar to Route 2 with the product vendors roles reversed. In this case the MCX Client Manufacturer is taking responsibility of the end system of MCX Client and UE being certified, and has a commercial agreement with the UE vendor to use their product as a certified UE platform. The certified UE platform shall have undertaken standard GCF Certification, and it is up to the MCX Client Manufacturer to ensure that the selected UE platform has the necessary features and functionality to support their MCX client functionality (ex LTE/5G bearers, QCI support, etc.)

While the UE supplier will be responsible for proper functionality of the UE platform, the MCX Client supplier will be at all times responsible for the ongoing compliance of the end product, throughout its entire life cycle.

Figure 6: Route 3 – Integration of an MCX Client on a GCF Certified device platform

4.2.4 Route 4: MCX only Client Certification

For MCX Client suppliers, there is a route to certification that allows their client to be certified as a commercial product and/or a Client Platform. Once certified, the MCX Client can be commercially procured for use on a GCF Certified UE. In the case of an MCX Client Platform (such as an SDK), these can be used to develop other MCX Clients with various functionalities that are enabled/disabled from the underlying platform. Any commercial product that utilises a MCX Client Platform, would need to undergo a separate certification to ensure the end product is meeting the requirements. This is required to ensure that the end product which may have certain features from the MCX Client Platform enabled or disabled, is properly developed. The end product certification testing for MCX can leverage much of the testing from the MCX Client Platform, and as a result, may have a quicker certification testing turnaround.

Process for undertaking a Mission Critical Services Client only certification:

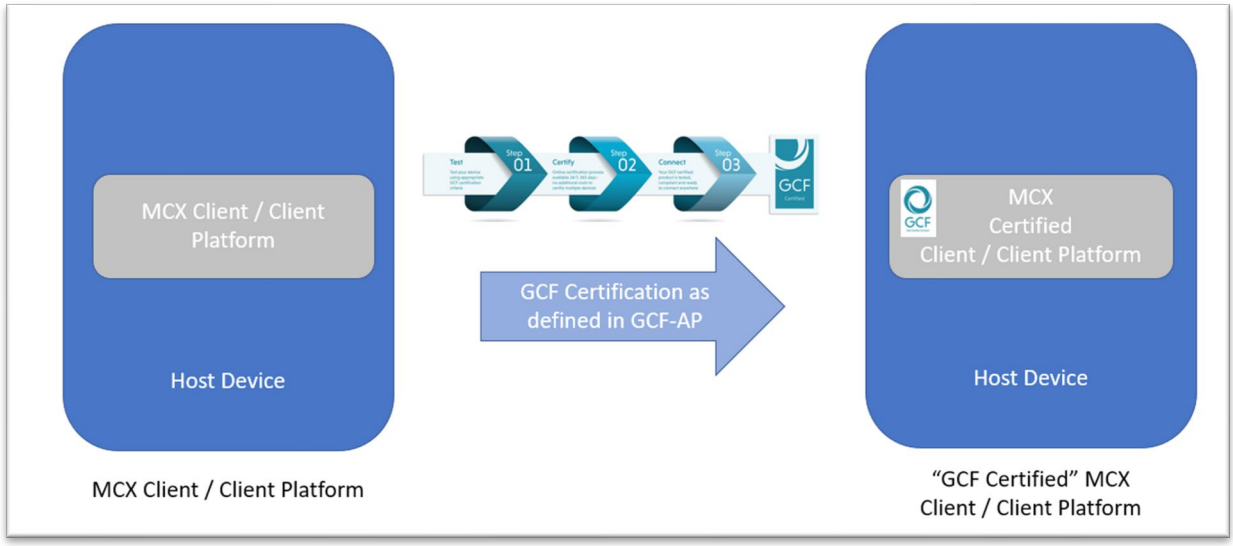

Figure 7: Route 4 – MCX Client Only Certification for commercialisation

Figure 8: Route 4 – MCX Client Only Certification as a Client Platform

5 MCS Product Procurement Scenarios

In order for Mission Critical Communications Operators to ensure they are acquiring certified products, several procurement scenarios have been developed that have been mapped to one of the Routes to Certification that the product supplier should follow. It is generally understood that a MCCO may be procuring one of the MCX product types from various different suppliers, or from a combination of suppliers. While these scenarios depict the procurement of single product type from a single vendor, these cases can be extrapolated to include multiple products of the same product type procured from multiple vendors.

For the purposes of certification, the following product types are captured in these scenarios:

- MCX Client
- MCX Capable UE
- MCX Server

In all instances the supplier(s) of the specific product type is responsible for the full scope of testing active in certification and as defined by the Certification Criteria in GCF-MCS PRD. If a desired product type certification is not yet available in the GCF Certification Programme (example MCX Server Certification), the MCCO should demand a commitment from the product type supplier to undertake certification of that product type, when certification of that product type is activated in the certification programme.

In addition, in all scenarios it is expected GCF Certification forms the **baseline level of requirements** needed to be achieved ***before*** MCCO network specific testing is conducted. This will ensure that any integration issues that are discovered can be easily isolated and is not related to compliance issues of the products. It also aims to minimize interoperability issues, as interoperability testing via IOP or Field Trials will have been conducted on the products during the certification stage.

It is important to note that if a MCCO procures a non-certified product type (example commercial UE that is not certified via one of the MCX Routes to Certification), then the risk introduced into the overall system by this product must be owned and managed by the MCCO via internal testing and approvals.

5.1 Single Vendor Scenario

In this scenario, the MCCO, or the designated entity contracted by the MCCO, is procuring all of the product types from one single supplier. The supplier of the product types is responsible for certification as follows:

- Certification of MCX Client & UE combination via Route#1 or Route#2
- Certification of MCX Servers (when available)

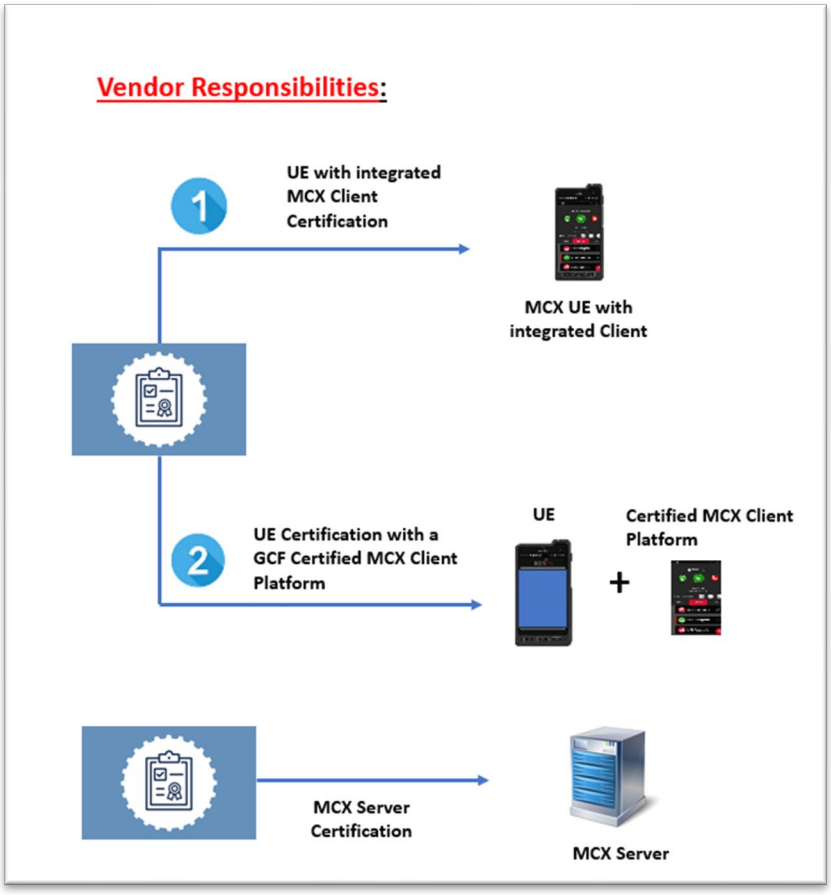

Figure 9: Single Vendor – MCX Client, UE & MCX Server Certification

5.2 Multi-Vendor Scenario: Vendor#1 supplies MCX Client & MCX Server; Vendor#2 supplies UE/Devices

In this scenario, the MCCO or the designated entity contracted by the MCCO, is procuring MCX Clients and Servers from one vendor, and MCX capable UEs from a second vendor. The supplier of each of the respective product types is responsible for certification as follows:

Vendor#1 Certification Responsibilities:

- Certification of MCX Client and/or Client Platform via Route#4
- Certification of MCX Servers (when available)

Vendor#2 Certification Responsibilities:

- Certification of the UE with MCX as a feature via Route#2

The certification of the UE can be done with any certified MCX Client or Client Platform, although the MCCO may prefer that the certification be done with the MCX Client and/or Client Platform that is supplied by Vendor#1.

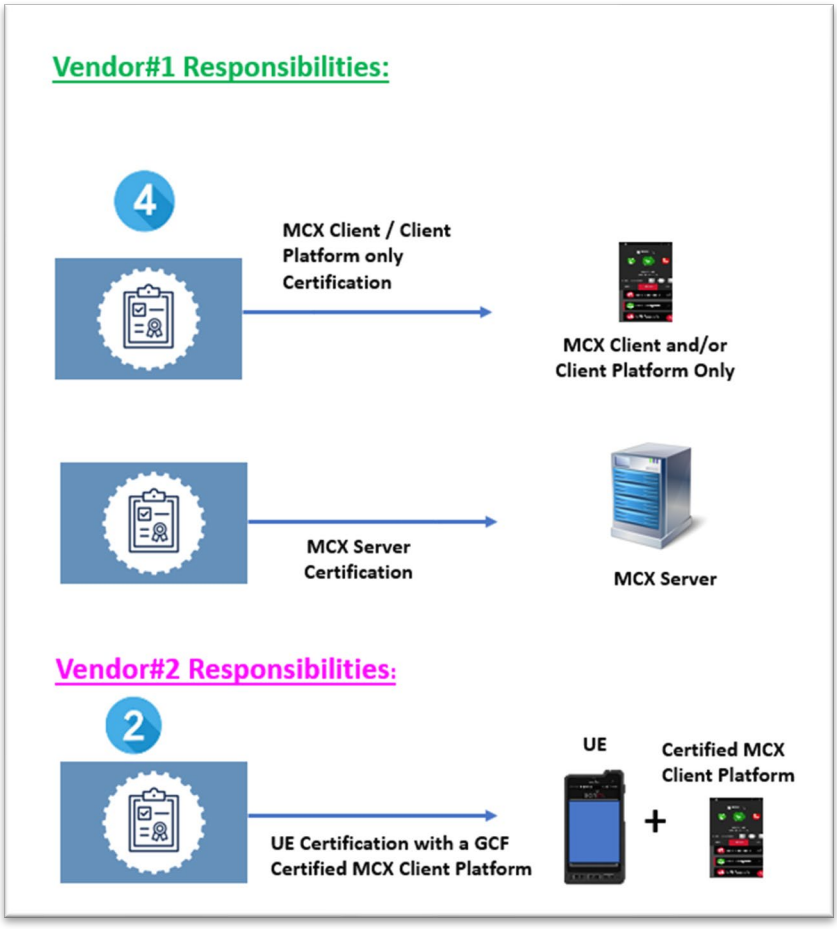

Figure 10: Multi-Vendor Scenario: Vendor#1 supplies MCX Client & Server; Vendor#2 supplies UE/Devices

5.3 Multi-Vendor Scenario: Vendor#1 supplies MCX Client & UE/Devices; Vendor#2 supplies MCX Server

In this scenario, the MCCO or the designated entity contracted by the MCCO, is procuring MCX Clients and UEs from one vendor, and MCX Servers from a different vendor. The supplier of each of the respective product types is responsible for certification as follows:

Vendor#1 Certification Responsibilities:

- Certification of MCX Client & UE combination via Route#1 or Route#2

Vendor#2 Certification Responsibilities:

- Certification of MCX Servers (when available)

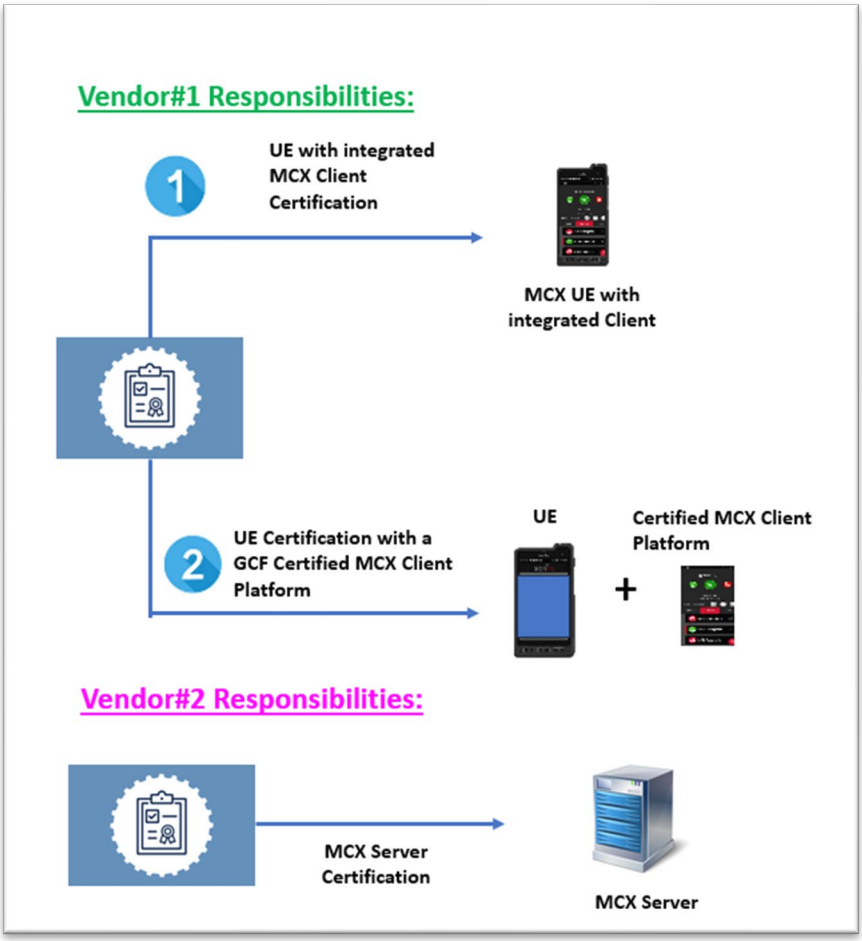

Figure 11: Multi-Vendor Scenario: Vendor#1 supplies MCX Client & UE/Devices; Vendor#2 supplies Server

5.4 Multi-Vendor Scenario: Vendor#1 supplies MCX Client; Vendor 2 suppliers UE/Devices; Vendor#3 supplies MCX Server

In this scenario, the MCCO or the designated entity contracted by the MCCO, is procuring MCX Clients, UEs, and MCX Servers from different vendors, with Vendor#1 supplying the MCX Client, Vendor#2 supplying the MCX capable UE, and Vendor#3 supplying the MCX Server. The supplier of each of the respective product types is responsible for certification as follows:

Vendor#1 Certification Responsibilities:

- Certification of MCX Client via Route#4

Vendor#2 Certification Responsibilities:

- Certification of the UE with MCX as a feature via Route#2

The certification of the UE can be done with any certified MCX Client or Client Platform, although the MCCO may prefer that the certification be done with the MCX Client and/or Client Platform that is supplied by Vendor#1.

Vendor#3 Certification Responsibilities:

- Certification of MCX Servers (when available)

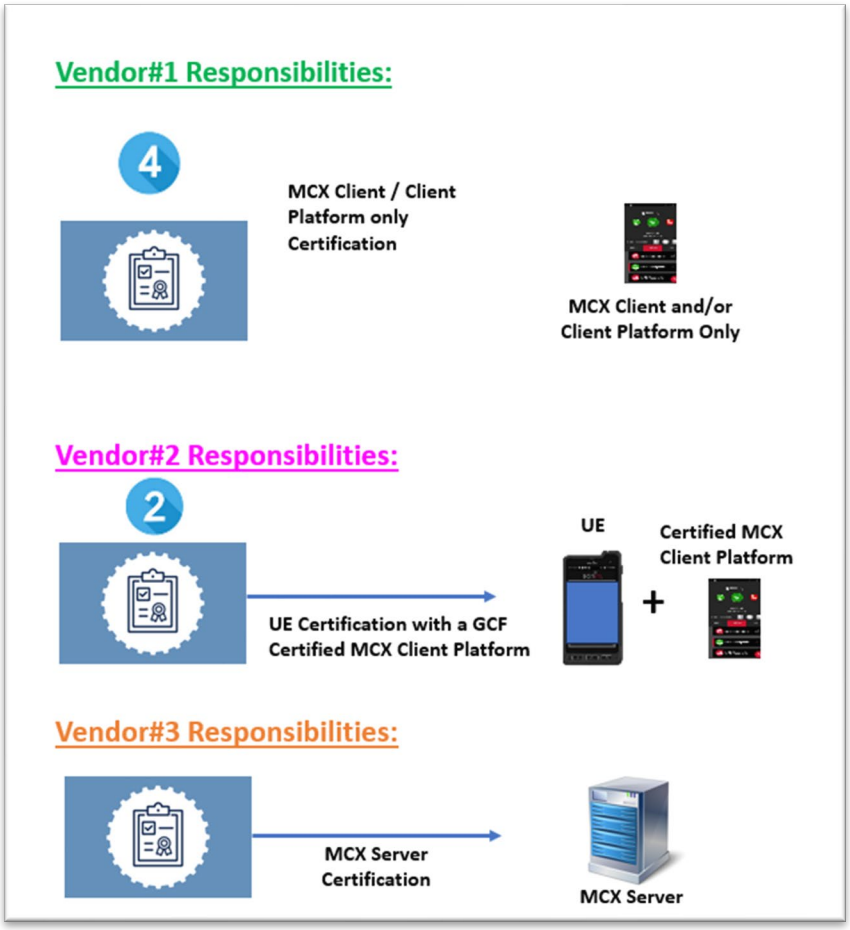

Figure 12: Multi-Vendor Scenario: Vendor#1 supplies MCX Client; Vendor#2 suppliers UE/Devices; Vendor#3 supplies MCX Server

6 Model Text for Contract Tenders

In order for the MCCO to have a baseline level of confidence that the products being procured are compliant to the standards, it is imperative for the contract tenders to indicate that certification of products to be procured is a mandatory requirement, whether they are being procured for internal testing, friendly user trials, and/or ultimately for commercial deployment.

To facilitate the Procurement Specialists of the MCCO, a model text that can be introduced into the contract tenders, that describes the minimum certification requirements for procured products, has been developed and is available for download from the TCCA's Legal and Regulatory Working Group (LRWG) Library:

https://tcca.info/tcca-recommended-procurement-text-library/

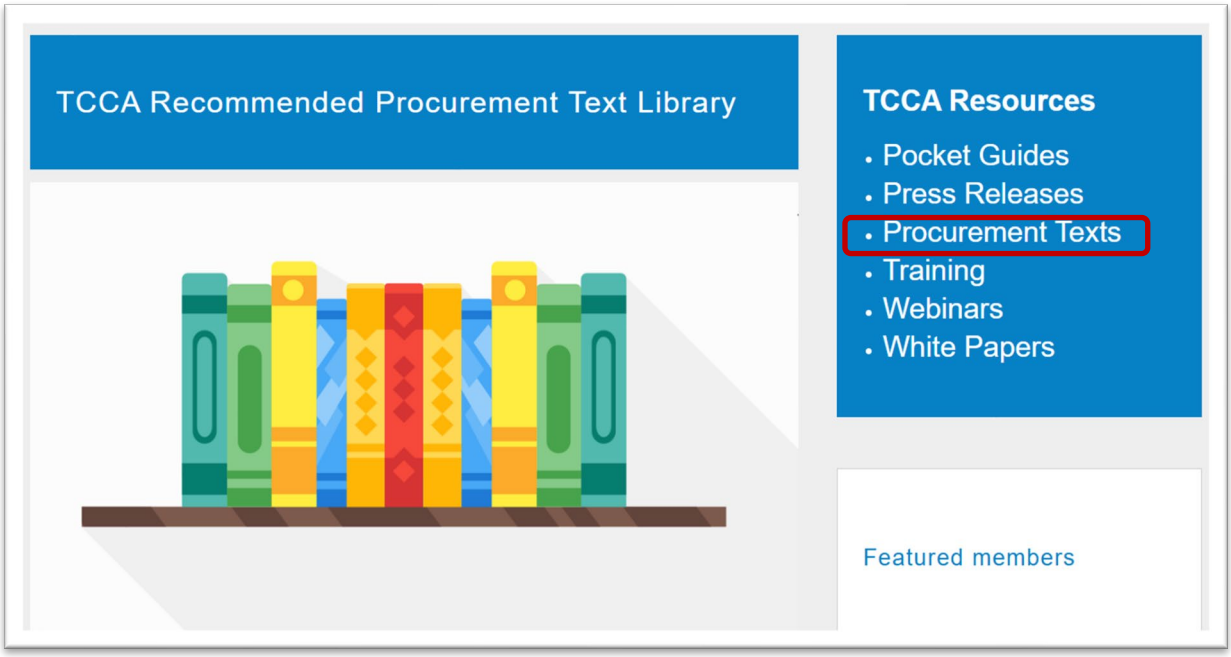

Figure 13: The TCCA LRWG Recommended Procurement Text Library

This library is accessible by any TCCA member and its content (including the model text) will be updated on an ongoing basis as certification requirements evolve over time. MCCOs are encouraged to use the standard template Model Text provided and may choose to customise it to fit their specific needs.

Below is the Model Text currently in place in the library, as an example and reference for the Procurement Specialists. In all cases, the MCCO is encouraged to download the latest version of the text for their contract tender purposes.

Suppliers must prove that broadband devices supporting group voice and data communications offered in response to this procurement provide Mission Critical Services (MCX) Client functionality and communication that is compliant with the 3GPP standard specifications for Mission Critical Services and broadband communication.

1 This proof is established by providing Certificates of Compliance issued by Global Certification Forum (GCF) for both the broadband device and the MCX client. Where the broadband device has an embedded MCX client the Certificates of Conformance for the device will cover the MCX client.

2 GCF certification for the MCX client, or MCX Client and device combination should following the process outlined in the latest version of the Mission Critical Services Certification Procedures Permanent Reference Document, (GCF-MCS), while the certification of the device (non-MCX) should follow the latest revision of the Applications Procedures (GCF-AP). Both documents can be accessed from the GCF Members' Portal:

https://www.globalcertificationforum.org/documents/official-documents/gcf-documents/gcf-reference-documents.html

3 A GCF recognised Assessment Capable Entity (ACE) must be used to determine the certification testing scope, i.e. the test plan, based on the features and functionality to be declared in the commercialised MCX product. A GCF Recognised Test Organisation (RTO), must be used to execute the test plan. A Certificate of Compliance issued by GCF following successful certification declaration submission and publication, must be presented as proof of certification.

4 The supplier must maintain their Compliance Folder with the relevant data filled Annexes required for certification as outlined in the GCF-MCS and GCF-AP PRDs throughout the lifecycle of the product, including performing any additional testing as required should the hardware and/or software impacting MCX change and broadband communication. The Mission Critical Communications Operator and/or Mobile Network Operator may check from time to time, and at its discretion, the contents of the Compliance Folder to ensure product compliancy.

5 This GCF MCX Certificate of Conformance may be in addition to other conformance requirements established by a mobile network operator. If GCF has not declared the relevant MCS Certification Activation Readiness by the time of procurement, the supplier must proactively ensure that certification is reached for the products within the scope of delivery and provide the Certificate without undue delay when the GCF has declared the relevant MCS Certification work items as Active. This can be achieved in the following ways:

1) The supplier must be a GCF manufacturer member in good standing and stay abreast of the latest developments of the Certification Programme including certification readiness timelines, and evolution to the certification criteria once activated.

1) The Mission Critical Communications Operator reserves the right to determine a payment amount related to this tender, as agreed in advance via bilateral discussions with the supplier, that may be withheld until the proof of certification as outlined above is provided.

Figure 13: Example of Model Text for MCX Contract Tenders

The text highlighted above contains several important elements that should be captured in the contract tender text:

1. This clause states the clear need for **Certificates of Compliance** from GCF as evidence of conformity

2. This clause refers to the latest **GCF MCS Certification Procedures and Version** that the Manufacturer should follow, and that is updated and managed by the Mission Critical Services Work Stream

3. This clause indicates the mandatory use of a **GCF RTO & ACE**

4. This clause captures the Manufacturer's responsibility for **Ongoing Compliance for product lifecycle**, including ensuring changes to hardware and software of the product are included in certification

5. This clause ensures the Manufacturer has in place **Proactive Measures for new Work Items** in Certification that may not yet have been activated but will be in the near future and that may be required by the MCCO to successfully provide the service

Get in touch

Since 1999 the Global Certification Forum (GCF), the industry recognised resource for trusted certification of connected devices in the consumer, professional and IoT spaces, has been delivering quality certification solutions that facilitate interoperable devices, networks, and services, enabling reliable and secure wireless communications globally.

Contact Us!

e: mcs@globalcertificationforum.org
w: https://www.globalcertificationforum.org/
LinkedIn: https://www.linkedin.com/company/global-certification-forum-gcf-ltd/

Global Certification Forum (GCF) Ltd
Suite 1, 7th Floor, 50 Broadway,
London
SW1H 0BL
United Kingdom