ETSI Plugtests Report V1.0.0 (2023-08)

3rd ETSI FRMCS Plugtests
Paris, France
03 July – 07 July 2023

Keywords

Testing, Interoperability, Mission-Critical, 5G, MCPTT, MCData, MCVideo, FRMCS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-préfecture de Grasse (06) N° 7803/88

Contents

Executive Summary

The capabilities of FRMCS including Mission Critical Push to Talk (MCPTT), Mission Critical Data (MCData) and Mission Critical Video (MCVideo) – together abbreviated as MCX services – were tested during the third FRMCS Plugtests from 03rd July to 07th July 2023 at the UIC Headquarter in Paris, France using a 5G test network. More than 300 test cases were executed between vendors, based on 3GPP Release-17.

The 3rd ETSI FRMCX Plugtests have concluded with a success rate of 86% of the executed tests in the validation of FRMCS vendor interoperability. More than 80 delegates participated during the 3rd FRMCS Plugtests event in Paris.

These tests are essential to ensure seamless access to FRMCS over 5G networks across different vendors' products and implementations.

The FRMCS Plugtests series is the first independent testing of railways and other mission critical services over 5G networks. The preparations for the third Plugtests started in April 2023, were followed by two weeks of integration with the test network in June 2023, a one week pre-testing in July 2023, and were finalized with a one week of face-to-face end to end interoperability testing with 5G test networks.

The tests were based on 3GPP Release-17 and more than 300 tests were executed between the different vendors in more than 80 test sessions. The test cases, which have been amended with additional test scenarios, will be included in a future new version of ETSI TS 103 564 (after the ETSI committee TCCE approval). Besides the MCPTT, MCData and MCVideo Application Servers and Clients, the testing also included, railways-oriented features and devices, railway emergency, etc. A test stream was dedicated for 3GPP RAN5 conformance testing.

The observations from the Plugtests events provide essential feedback to 3GPP Working Groups as work continues in 3GPP and ETSI FRMCS specifications.

The testing during the 3rd FRMCS Plugtests was complemented by an observer program with presentations, round-table discussions and demos for the observers.

This third FRMCS Plugtests was organized by ETSI with the support of the European Commission, EFTA, TCCA and UIC.

The Plugtests event was a pure interoperability testing event, and no products were certified.

The next FRMCS Plugtests event are planned for June 2024.

The companies participating in this FRMCS Plugtests have been testing the following equipment in the indicated Test Streams:

FRMCS/MCX Application Servers:	Stream A FRMCS over 5G	Stream B Conformance Testing
Alea	X	
Consort Digital	X	
Kontron	X	
MC Labs	X	X
Nemergent	X	
Nokia	X	
Tassta	X	
Valid8	X	

FRMCS/MCX Clients:	Stream A FRMCS over 5G	Stream B Conformance Testing
Alea	X	
Alstom	X	X
Atos	X	
Consort Digital	X	

FRMCS/MCX Clients:	Stream A FRMCS over 5G	Stream B Conformance Testing
Funkwerk	X	
Kontron	X	X
MC Labs	X	X
Nemergent	X	X
Tassta	X	
Softil	X	
Teltronic	X	

User Equipment (UE):	Stream A FRMCS over 5G
Alstom (On-board Gateway)	X
Alstom (Track-side Gateway)	X
Consort Digital (CabRadio)	X
Crosscall (5G Device)	X
Funkwerk (5G Device)	X
Funkwerk (CabRadio)	X
Siemens (CabRadio)	X

Next Generation Node B (gNB):	Stream A FRMCS over 5G
Athonet	X

5G Core:	Stream A FRMCS over 5G
Athonet	X

Dispatcher:	Stream A FRMCS over 5G	Stream B Conformance Testing
Atos	X	
Consort Digital	X	
Frequentis	X	
Kontron	X	
RideOnTrack	X	
Softil	X	
Teltronic	X	

Test Tool Vendors:	Stream B Conformance Testing
MCS-TaaSting	X
Valid8	X

The following observer organisations participated in this Plugtests:

- A.S.T.R.I.D, Public saftey network operator, Belgium

- Cybersecurity and Infractructure Security Agency / Department of Homeland Security, USA
- Erillisverkot, Public saftey network operator, Finland
- Home Office, United Kingdom
- French Ministry of Interior, France
- ProRail, Netherlands
- SMIT, Information technology and development center of the Ministry of the Interior, Estonia
- SNCF Reseau, Railway operator research, France
- DSB, Norwegian Directorate for Civil Protection, Norway
- TCCA
- UIC Union Internationale des Chemins de Fer

1 Introduction

Mission Critical Push To Talk (MCPTT) is a 3GPP standardized voice service for mobile radio systems which ensures that LTE (and 5G) systems support mission-critical communications.

The Global Mission-Critical Communication Market was valued at USD 17.03 Billion in 2022 and is estimated to reach USD 27.87 Billion by 2028 growing at a CAGR of 8.6% during the forecast period 2022–2028, according to the market research. The global train control and management systems market is expected to grow from $3.73 billion in 2022 to $3.99 billion in 2023 at a compound annual growth rate (CAGR) of 7.2%. The nationwide rollouts in the European countries are expected to trigger significant large-scale investments in mission-critical 5G.

Mission Critical Push To Talk (MCPTT) was the first of a number of Mission Critical features which was standardized by 3GPP in Release-13. Mission Critical Video and Mission Critical Data were standardized in Release-14. With the standardization of MCX (Mission-Critical PTT, Video & Data), FRMCS, and other critical communications features by 3GPP, 5G networks are increasingly gaining recognition as an all-inclusive communications platform for public safety, railways, utilities, maritime and other critical communications sectors.

Preparations for the 3rd ETSI FRMCS Plugtests event started in April 2023 with the registrations of vendors and observers. During bi-weekly conference calls from April to June 2023 the setup of the tests, the test specification and organizational issues were agreed between the participants. Before the main event, the vendors have done integration with test network and remote pre-testing of their implementations via VPN tunnels which connected their labs to a central exchange hub.

All the information required to organise and manage the 3rd FRMCS Plugtests event was compiled and shared with participants in a dedicated private WIKI which was put in place by ETSI. All participants were provided with credentials that allowed them to access and update their details. All the information presented in this document has been extracted from the 3rd FRMCS Plugtests event wiki: https://wiki.plugtests.net/3rd-FRMCS-Plugtests/index.php (login required).

Clause 4 describes the management of the Plugtests event.

The following equipment was tested – please see also clause 5:

- FRMCS/MCX Application Servers (MCX AS)
- FRMCS/MCX Clients
- Next Generation Node B (gNB)
- User Equipment (UE)
- 5G Core (5GC)
- MCX Conformance Test Tools
- Dispatchers
- CabRadios
- OB-GW (On-Board Gateway)
- TS-GW (Trackside Gateway)

In this Plugtests the railways-oriented Application Servers and Clients were evaluated in a dedicated test stream over 5G test network. This Stream A was available for vendors to evaluate their equipment for end-to-end interoperability testing over 5G networks.

A dedicated Test Tools test stream (Stream B) was available for test tool vendors and other vendors to check their tools and the conformance of the implementations with these test tools. All MCX client vendors were encouraged to check their implementations against these conformance test tools.

The remote test infrastructure is described in clause 6; the test procedures are described in clause 7.

The vendors and ETSI have set up VPN-Tunnels from the vendors' premises to the ETSI VPN hub. This allowed the vendors to start integration work and pre-testing of FRMCS services before the Plugtests week.

For the 3rd FRMCS Plugtests 8 additional test case scenarios were developed by ETSI. In total, the FRMCS test specification has now more than 350 test cases. See clause 8. An updated version of the test specification will be published as a new version of ETSI document ETSI TS 103 564 (after ETSI TC TCCE approval).

More than 300 tests were conducted by the vendors. 86.0% of the tests were successful, the remaining 14.0% failed for various reasons. The detailed results of the tests are available for the involved vendors in these test sessions but are not disclosed to the other vendors or to the public. All participants had to sign a Non-Disclosure Agreement and Rules of Engagement before joining the Plugtests event. The statistics of the test results are listed in clause 9.

The failed tests are very valuable because they give the vendors information on how to improve their implementations. They also help to discover errors or ambiguities in the standards and to clarify and improve the specifications.

The next FRMCS#4 Plugtests sessions are planned for Q2 2024. Vendors and observers who have not participated in the previous FRMCS Plugtests events are welcomed and encouraged to join the next FRMCS Plugtests event.

2 References

The following documents have been used as references in the Plugtests. The participants in the Plugtests agreed on a set of specific documents and Release 16 versions for the sixth MCX Plugtests. Please see also the test specification document for the references.

[1] ETSI TS 103 564: Plugtests scenarios for Mission Critical Services.

[2] 3GPP TS 22.179: Mission Critical Push to Talk (MCPTT) over LTE.

[3] 3GPP TS 23.280: Common functional architecture to support mission critical services.

[4] 3GPP TS 23.379: Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT)

[5] 3GPP TS 24.229: IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).

[6] 3GPP TS 24.281: Mission Critical Video (MCVideo) signalling control.

[7] 3GPP TS 24.282: Mission Critical Data (MCData) signalling control.

[8] 3GPP TS 24.379: Mission Critical Push To Talk (MCPTT) call control.

[9] 3GPP TS 24.380: Mission Critical Push To Talk (MCPTT) media plane control.

[10] 3GPP TS 24.481: Mission Critical Services (MCS) group management.

[11] 3GPP TS 24.482: Mission Critical Services (MCS) identity management.

[12] 3GPP TS 24.483: Mission Critical Services (MCS) Management Object (MO).

[13] 3GPP TS 24.484: Mission Critical Services (MCS) configuration management.

[14] 3GPP TS 24.581: Mission Critical Video (MCVideo) media plane control.

[15] 3GPP TS 24.582: Mission Critical Data (MCData) media plane control.

[16] 3GPP TS 26.179: Mission Critical Push To Talk (MCPTT); Codecs and media handling.

[17] 3GPP TS 26.346: Multimedia Broadcast/Multicast Service (MBMS).

[18] 3GPP TS 29.212: Policy and Charging Control (PCC).

[19] 3GPP TS 29.214: Policy and Charging Control over Rx reference point.

[20] 3GPP TS 29.468: Group Communication System Enablers for LTE(GCSE_LTE); MB2 reference point.

[21] 3GPP TS 33.180: Security of the mission critical service.

[22] IETF RFC 3515: The Session Initiation Protocol (SIP) Refer Method.

[23] IETF RFC 3856: A Presence Event Package for the Session Initiation Protocol (SIP).

[24] IETF RFC 3903: Session Initiation Protocol (SIP) Extension or Event State Publication.

[25] IETF RFC 4488: Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription,.

[26] IETF RFC 4825: The Extensible Markup Language (XML) Configuration Access Protocol (XCAP).

[27] IETF RFC 5366: Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP).

[28] IETF RFC 5373: Requesting Answering Modes for the Session Initiation Protocol (SIP).

[29] IETF RFC 5875: An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Diff Event Package.

[30] IETF RFC 6135: An Alternative Connection Model for the Message Session Relay Protocol (MSRP).

[31] IETF RFC 6665: SIP-Specific Event Notification.

[32] IETF RFC 7647: Clarifications for the use of REFER with RFC6665.

[33] OMA. OMA-TS-XDM_Core-V2_1-20120403-A: XML Document Management (XDM) Specification.

[34] OMA. OMA-TS-XDM_Group-V1_1_1-20170124-A: Group XDM Specification.

[35] IETF RFC 7230: Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing.

[36] IETF RFC 5246: The Transport Layer Security (TLS).

[37] IETF RFC 6101: The Secure Sockets Layer (SSL).

[38] IETF RFC 4975: The Message Session Relay Protocol (MSRP).

[39] 3GPP TR 21.905: Vocabulary for 3GPP Specifications.

3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [39] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [39].

5GC	5G Core
5GS	5G System
AMR	Adaptative Multi-Rate Audio Codec
AMR-WB	Adaptative Multi-Rate Audio Codec Wideband
APP	Application
AS	Application Server
CMS	Configuration Management Server
CSC	Common Services Core
CSCF	Call Session Control Function
CSK	Client-Server Key
DUT	Device Under Test
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
ETSI	European Telecommunications Standard Institute
EUT	Equipment Under Test
FA	Functional Alias
FD	File Distribution
FE	Functional Element
FRMCS	Future Railway Mobile Communication System
GCSE	Group Communication Service Enabler
GMK	Group Master Key
GMS	Group Management Server
gNB	g Node B (5G base station)
iFC	Initial Filter Criteria
IFS	Interoperable Functions Statement
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IdMS	Identity Management Server
IWF	Interworking Function
KMS	Key Management Server
MBMS	Multimedia Broadcast and Multicast Service
MCData	Mission Critical Data
MCPTT ID	MCPTT user identity
MCPTT	Mission Critical Push-To-Talk
MCVideo	Mission Critical Video
MCX	Mission Critical Services (X stands for PTT, Data and Video)
OAM	Operation and Maintenance
OB-GW	On-board Gateway
OTT	Over the Top
P25	Project 25
PCC	Policy and Charging Control
PCRF	Policy and Charging Rules Function
PES	Pre-established Sessions
PSI	Public Service Identity
PSTA	Public Safety Technology Association
PTT	Push-To-Talk
ProSe	Proximity-based Services
RAN	Radio Access Network
RTP	Real-time Transport Protocol
SDS	Short Data Service
SIP	Session Initiation Protocol
SPK	Signalling Protection Key
TCCA	The Critical Communications Association
TD	Test Description
TR	Technical Recommendation

TRT	Test Reporting Tool
TS	Technical Specification
TS-GW	Track-side Gateway
UE	User Equipment
UIC	International Union of Railways (Union Internationale des Chemins de fer)
VPN	Virtual Private Network

4 Technical and Project Management

4.1 Scope

The main goal of the FRMCS Plugtests was testing the interoperability of the MCPTT, MCData and MCVideo ecosystem signalling and media plane at different levels for railway related FRMCS functionalities.

The basic scenario tested comprised MCX application server(s) -both controlling and participating- with integrated SIP Core and MCX clients, 5G access network with and without MCX required PCC capabilities and UEs. The following figure (Fig 1) illustrates the basic test infrastructure.

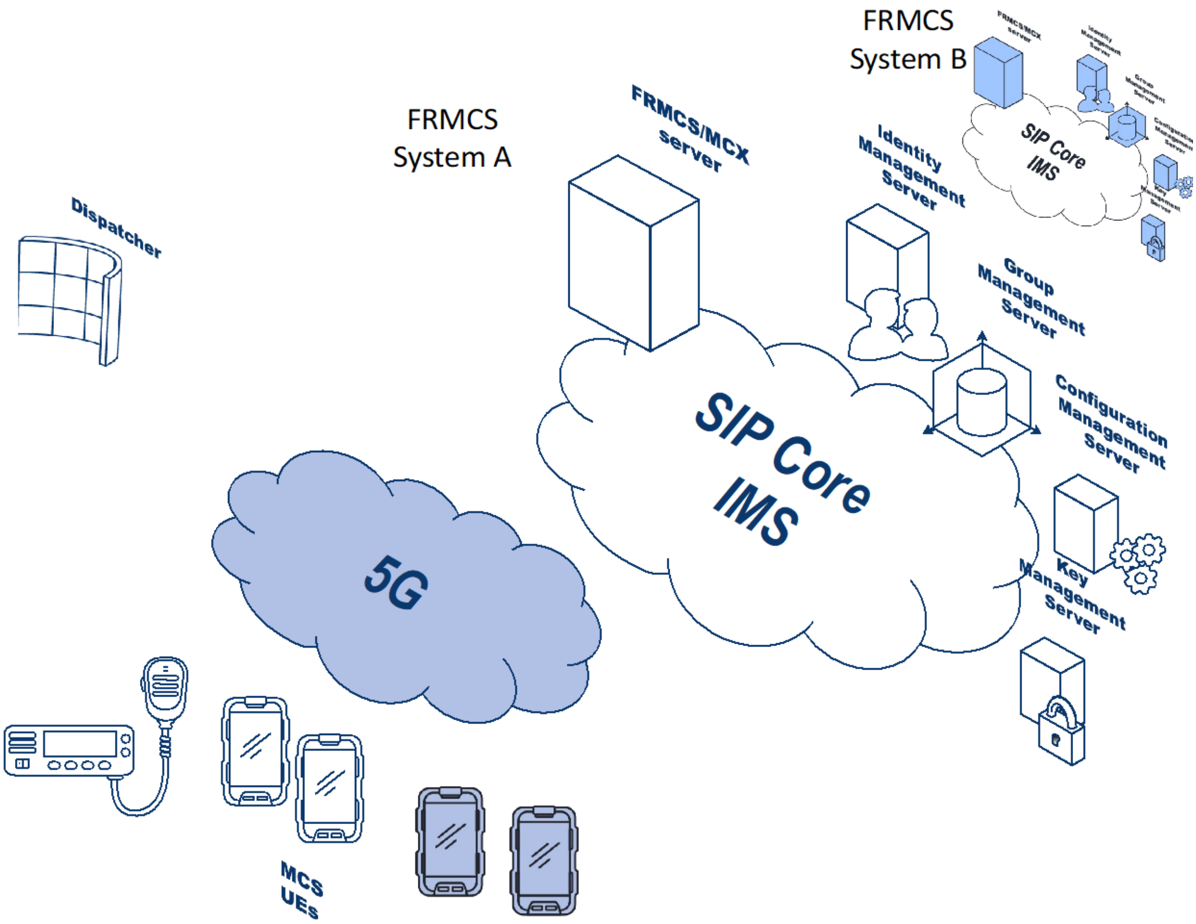


Figure 1. Typical MCPTT/MCData/MCVideo scenario to be considered in the Plugtests

In the scope of this Plugtests event, the following high level test objectives were performed

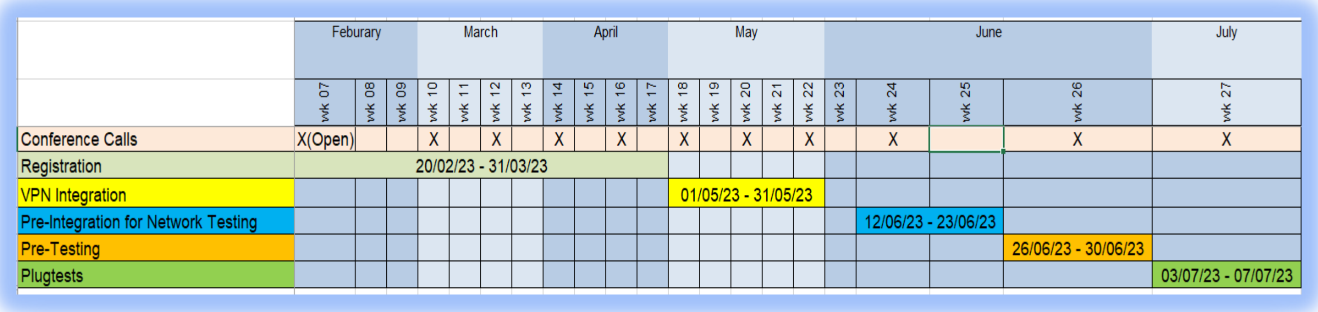
- **Connectivity (CONN)**: Tests covered connectivity between functional elements at different levels including Access Network (5G), IP Network, SIP/IMS and MCPTT/MCData/MCVideo Application level. Tests at IP layer targeted pure OTT connectivity regardless the underlying access network. SIP connectivity tests checked proper deployment of MCX AS over the selected SIP Core/IMS so that all SIP messages were successfully delivered from MCX Clients to Participating/Controlling MCPTT Servers and vice versa. In this 3rd Plugtests, again, some AS vendors provided their own built in SIP/IMS cores so that Clients registered into different cores depending of the specific test session. Application level refers to e2e signalling, media, floor controlling (and other involved) protocols in use. Although for this Plugtests participants were encouraged to carry on CONN tests over Mission Critical 5G for unicast and Mission Critical 5G, most tests used the OTT (i.e. using WIFI / wired connections) one for its flexibility and the possibility of scheduling parallel test easily. MCData and MCVideo features were mostly analysed in test cases associated to the CONN objective while sibling procedures (i.e. registration to different MCPTT/MCData/MCVideo servers) were carried out when needed.
- **Floor Controlling (FC):** Apart from the basic Floor Controlling procedures considered during the first CONN objective, FC comprised comprehensive interoperability analysis of more complex interactions, including

prioritization and pre-emptive mechanisms. Additional test cases comprising more advanced floor controlling (i.e. timeouts and revokes) were evaluated.

- **Registration and authorization (REGAUTH)**: Comprised MCX Client registration.
- **Affiliation (AFFIL)**: Comprised MCX Client explicit and implicite affiliation
- **Server-to-server communications (S2S)**: Controlling to non-controlling interface for temporary groups in different trust configurations.
- **Function Alias (FA)**:Activating and deactivating functional alias.
- **User and group regrouping using preconfigured group (RegrPrec):** as an alternative to OAM (GMS) creation.
- **FRMCS**: Railway oriented features were implemented to test functional aliases, IP Connectivity, etc.
- **Observer Test Scenarios**: more complex test scenarios which have been developed by observers.
- **Inter MCX**: MCPTT/MCVideo connectivity test cases were used to test interworking between application servers.

4.2 Timeline

The preparation was run through different phases as described in the figure below.



	Feburary			March				April				May					June				July
	wk 07	wk 08	wk 09	wk 10	wk 11	wk 12	wk 13	wk 14	wk 15	wk 16	wk 17	wk 18	wk 19	wk 20	wk 21	wk 22	wk 23	wk 24	wk 25	wk 26	wk 27
Conference Calls	X(Open)			X		X		X		X		X		X		X		X		X	X
Registration	20/02/23 - 31/03/23																				
VPN Integration												01/05/23 - 31/05/23									
Pre-Integration for Network Testing																		12/06/23 - 23/06/23			
Pre-Testing																				26/06/23 - 30/06/23	
Plugtests																					03/07/23 - 07/07/23

Figure 2. Plugtests event timeline

Registration to the FRMCS Plugtests event was open from 20th February 2023 to 31st March 2023 to any organisation willing to participate in testing the FRMCS Ecosystem. A total of 90 people were finally involved in the Plugtests event.

The following clauses describe the different phases of the Plugtests event preparation. It is worth noting that since the start of the documentation phase until the first week of the Plugtests event, bi-weekly conference calls were run among organisers and participants to discuss and track the progress, anticipate and solve technical issues, review the test plan, etc.

4.2.1 Documentation

Once the registration to the Plugtests event was closed, the following documentation activities were launched in parallel:

1) EUT Documentation

Participants documented their EUTs, by providing the information directly to the Plugtests event team. The Plugtests event team compiled the final EUT table for all the participating vendors and was appended to the Plugtests event Test Plan,

All the information described above was made available in the Plugtests event WIKI, so that it could be easily maintained and consumed by participants.

2) Test Plan Development

The Test Plan development was led by ETSI Centre for Testing and Interoperability following the methodology defined by 3GPP TSG SA6 and 3GPP TSG CT1. The Test Plan was scoped around 3GPP Test Specification Release-17 capabilities and concentrated on the features supported by the implementations attending the Plugtests event.

The Test Plan was developed and consolidated in an iterative way, taking into account input and feedback received from Plugtests event participants. See details in clause 8.

4.2.2 Integration & pre-testing

From 01st May to 31st May 2023, participants connected their equipment's with ETSI HIVE infrastructure to collaboratively run the pretesting remotely.

From 12th June to 23rd June 2023, participants connected their equipment's with Athonet 5G network to collaboratively run the Interoperability Test Sessions remotely. Over the top IP based testing was performed by during the pretesting phase from 26th June to 30th June 2023.

Participants connected their implementations remotely to the Plugtests event infrastructure, known as HIVE: Hub for Interoperability and Validation at ETSI. Participants also integrated their equipment with 5G test networks to participate in the streams A.

During this phase, up to 17 remote labs connected to HIVE and each of them was allocated a dedicated network. The interconnection of remote labs allowed running integration and pre-testing tasks remotely among any combination of participating EUTs, in order to ensure an efficient use of the Plugtests event time and smoother Interoperability test sessions.

A VPN connection to the HIVE was highly recommended for participants providing FRMCS/MCX Application Servers, FMRCS/MCX Clients and Test Tools for first connectivity tests, trouble shooting and infrastructure access purposes.

Additional details on the remote test infrastructure, remote integration and pre-testing procedures are provided in Clauses 6 and 7.

For the 5G testing at the UIC in Paris, MCX AS Servers have been connected remotely to the 5G test systems.

During this phase, the bi-weekly conference calls were continued among organisers and participants to synchronise, track progress and get ready for the on-site phase.

4.2.3 Plugtests event

From 3rd July to 7 July 2023 the Plugtests participants met in the UIC headquarter in Paris, France and tested with each other over the Radio Interface.

The scheduling of individual test combinations was done randomly using ETSI Test Reporting tool as well as participants agreed test session slots between themselves. The schedule was adapted during the test session slots on a per need basis.

4.3 Tools

4.3.1 Plugtests event WIKI

The Plugtests event WIKI was the main source of information for the MCX Plugtests event, from logistics aspects to testing procedures. Access to the WIKI was restricted to participating companies.

The main technical information provided in the wiki was organised as follows:

- **Event Information** – Logistics aspects of the Plugtests event.
- **Visa Information** – Visa related information was provided for vendors require visa for travel.
- **List of Participants** – List of participants in the event.
- **Schedule –** Complete schedule of the event.

- **Observer Program** – Information about the Observer presentations, round table discussions and Observer demo during the Plugtests event.
- **Test Tools** – Information from the Test Tool vendors about what kind of tests they are offering for the Plugtests.
- **Test Network Information –**5G test network information.
- **IT Infrastructure** - HIVE connection request tool, and remote connections status overview.
- **Specifications -** High Level Test Scope including the test specification and reference to 3GPP and IETF specifications.
- **Equipment under Test** - Participating EUTs overview and contact information.
- **Provisioning Information -** Pre-configured parameters for EUTs.
- **Test Reporting Tool** - Documentation of the Test Reporting Tool.
- **Conf Calls** - Calendar, logistics, agendas and minutes of the bi-weekly conference calls run during the remote integration and pre-testing phase.
- **Observations** - Issues found during Plugtests event.
- **Host Information** – Information about the equipment available at host University of Malaga.
- **Networking Dinner** – Information regarding networking dinner.

In addition, Slack was used among the participants to communicate with each other during the pre-testing phase and Test Sessions, include their remote colleagues (back-office support) in the discussions.

4.3.2 Test Reporting Tool (TRT)

The Test Reporting Tool guides participants through the Test Plan test cases during the pre-testing and main Test Sessions. It allows creating Test Session Reports compiling detailed results for the individual scheduled Test Sessions.

Only the companies providing the EUTs for each specific Test Session combination have access to their Test Session Reports contents and specific results. All companies involved in a specific session and who have entered the test results were required to verify and approve the reported results at the end of each session. Only test report which has been approved by all involved parties are considered as valid.

Another interesting feature of this tool is the ability to generate real-time stats (aggregated data) of the reported results, per test case, test group, test session or overall results. These stats are available to all participants and organisers and allow tracking the progress of the testing with different levels of granularity, which is extremely useful to analyse the results.

5 Equipment Under Test

The tables below summarise the different EUTs provided by the Plugtests event participants:

5.1 FRMCS/MCX Application Servers

Organisation	Support
Alea	MCPTT, MCDATA, MCVIDEO
Consort Digital	MCPTT, MCDATA
Kontron	MCPTT, MCDATA
MC Labs	MCPTT, MCVIDEO
Nemergent	MCPTT, MCDATA, MCVIDEO
Nokia	MCPTT, MCDATA, MCVIDEO
Tassta	MCPTT, MCDATA, MCVIDEO
Valid8	MCPTT, MCDATA, MCVIDEO

Table 1. FRMCS/MCX Application Servers Under Test

5.2 FRMCS/MCX Clients

Organisation	Support
Alea	MCPTT, MCDATA, MCVIDEO
Alstom	MCDATA, ON BOARD GATEWAY, TRACK SIDE GATEWAY
Atos	MCPTT, MCDATA, MCVIDEO
Consort Digital	MCPTT, MCDATA
Funkwerk	MCPTT, MCDATA, MCVIDEO
Kontron	MCPTT, MCDATA
MC Labs	MCPTT, MCVIDEO
Nemergent	MCPTT, MCDATA, MCVIDEO
Tassta	MCPTT, MCDATA, MCVIDEO
Teltronic	MCPTT, MCDATA

Table 2. FRMCS/MCX Clients Under Test

5.3 Dispatcher (DISP)

Organisation	Support
Atos	MCPTT, MCDATA, MCVIDEO
Consort Digital	MCPTT, MCDATA, MCVIDEO
Frequentis	MCPTT, MCDATA, MCVIDEO
Kontron	MCPTT, MCDATA
RideOnTrack	MCPTT
Softil	MCPTT, MCDATA, MCVIDEO
Teltronic	MCPTT, MCDATA

Table 3. Dispatcher (DISP) Under Test

5.4 5G Core (5GC)

Organisation	Support
Athonet	

Table 4. 5G Core Under Test

5.5 5G New Radio (5GNR)

Organisation	Support
Athonet	

Table 5. 5G NR Under Test

5.6 User Equipment (UE)

Organisation	Support
Alstom	On-board Gateway
Alstom	Track-side Gateway
Consort Digital	Cab radio
Crosscall	5G Device
Funkwerk	5G Device
Funkwerk	Cab radio
Siemens	Cab radio

Table 6. User Equipment Under Test

5.7 Test Tools

Organisation	Support
MCS-TaaSting	MCX Conformance Tester
Valid8	MCX Conformance Tester

Table 7. Testers Under Test

6 Test Infrastructure

6.1 Remote Test Infrastructure

The remote testing and pre-testing phase were enabled by the setup as shown in Figure 4:

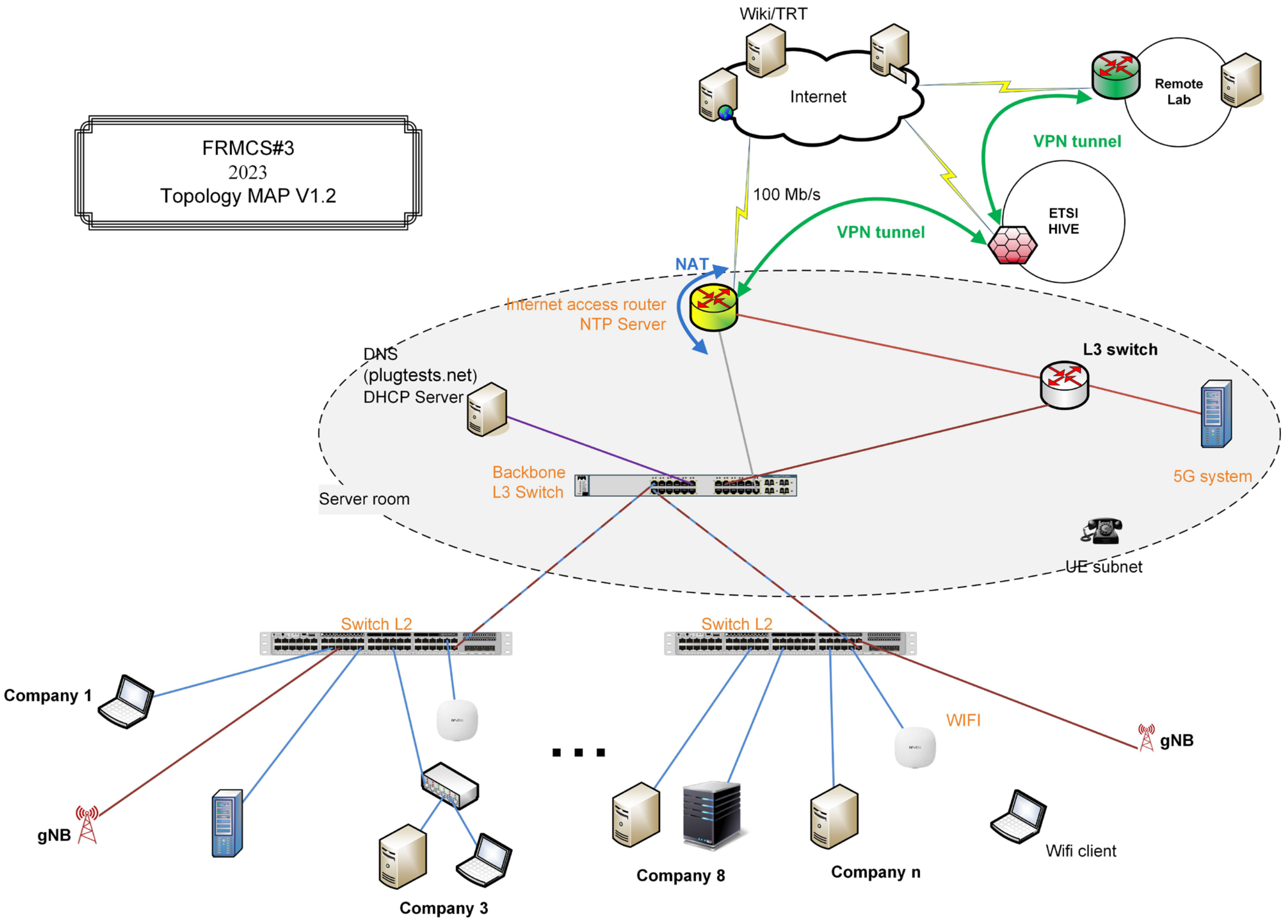


Figure 3. Remote Test Infrastructure

Once HIVE was deployed, a number of VPN tunnels were created to interconnect the equipment of the participants where the EUTs were running.

A total of 17 Remote Labs connected to the setup described above as a participant's lab.

7 Test Procedures

7.1 Remote Integration & Pre-testing Procedure

During the remote integration and pre-testing phase the following procedures were followed by the participating Equipment Under Test. Once the EUT documentation and HIVE connection had been successfully completed, the test cases from the test specifications were executed as part of the pre-testing

The progress of these procedures for the different combinations of EUTs was captured in the reporting function of TRT. The following Pre-Testing configurations were used in the pretesting phase

Config Name	Pre-testing Configuration
PreTest-OTT-CabRadio	CabRadio + FRMCS AS
PreTest-OTT-Client	FRMCS Client + FRMCS AS
PreTest-OTT-Dispatcher	FRMCS AS + Dispatcher

Table 8. Pre-testing Configuration

7.2 Interoperability Testing Procedure

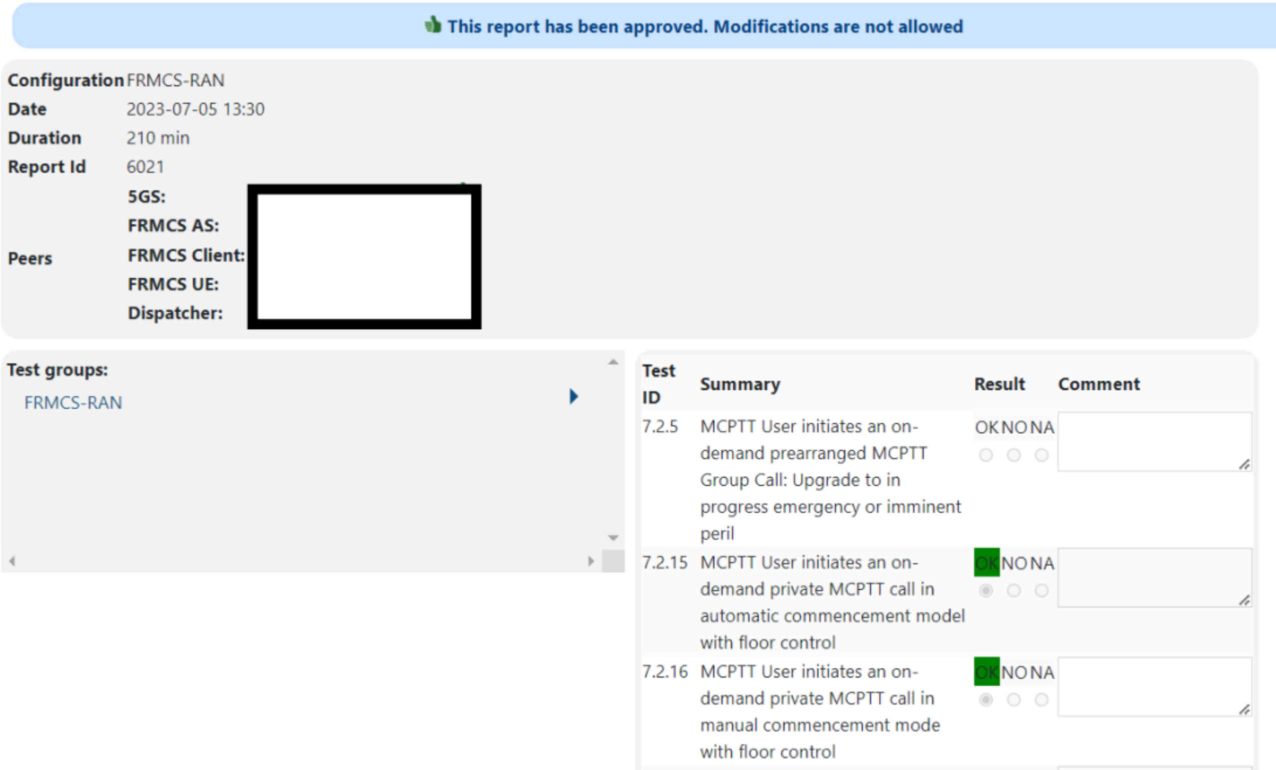
During the Plugtests event, a daily Test Session Schedule was added and shared via the TRT. Test Sessions were organised in several parallel tracks, ensuring that all participants had at least one Test Session scheduled any time. The different test configurations were used for the main event.

Config Name	Main Test Configuration
FRMCS-IPConn	TS GW + FRMCS AS + Dispatcher
FRMCS-RAN	5GS + FRMCS Client + FRMCS AS + FRMCS UE + Dispatcher
FRMCS-RAN-CabRadio	5GS + CabRadio + FRMCS AS + Dispatcher
FRMCS-RAN-Multi-AS	5GS + FRMCS Client + FRMCS AS + FRMCS AS + FRMCS UE + Dispatcher
FRMCS-RAN-Multi-Client	5GS + FRMCS Client + FRMCS AS + FRMCS Client + FRMCS UE + FRMCS UE + Dispatcher
Conformance-AS	Tester + FRMCS AS
Conformance-Client	Tester + FRMCS Client

Table 9. Main Test Configurations

During each test session, for each tested combinations the Interoperability testing procedure was as follows:

1. The participating vendors opened the Test Session Report and the Test Plan.



This report has been approved. Modifications are not allowed

Configuration FRMCS-RAN
Date 2023-07-05 13:30
Duration 210 min
Report Id 6021
Peers 5GS: FRMCS AS: FRMCS Client: FRMCS UE: Dispatcher: [redacted]

Test groups:
FRMCS-RAN

Test ID	Summary	Result	Comment
7.2.5	MCPTT User initiates an on-demand prearranged MCPTT Group Call: Upgrade to in progress emergency or imminent peril	OK NO NA	
7.2.15	MCPTT User initiates an on-demand private MCPTT call in automatic commencement model with floor control	OK NO NA	
7.2.16	MCPTT User initiates an on-demand private MCPTT call in manual commencement mode with floor control	OK NO NA	

Figure 4. Test Session Report

2. For each Test in the Test Plan:

   a. The corresponding Test Description and EUT Configuration were followed.

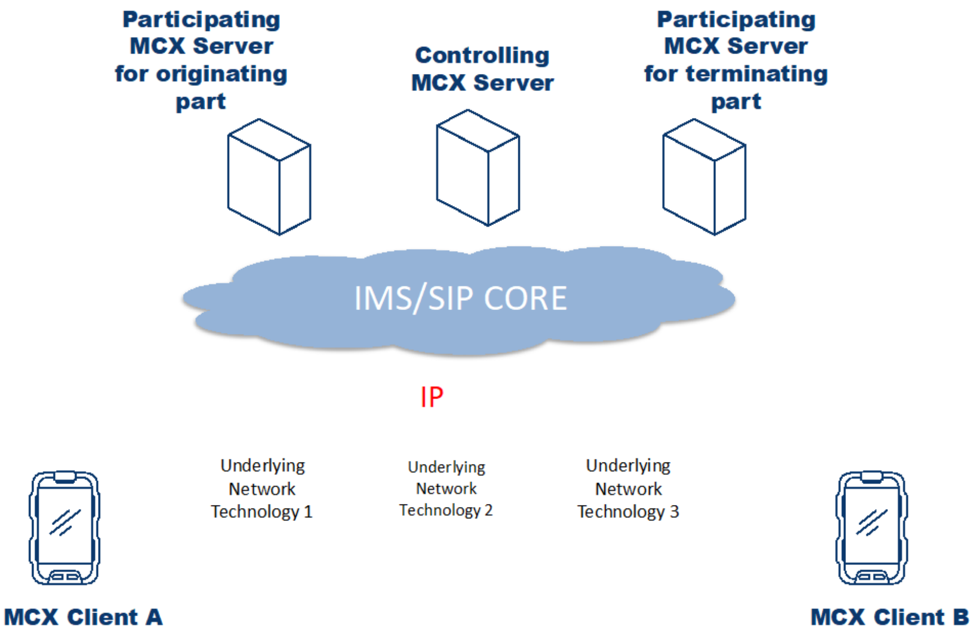


Figure 5. System Under Test (SUT) Configuration – MCX example

Interoperability Test Description			
Identifier	CONN/ONN/GROUP/PREA/ONDEM/NFC/01		
Test Objective	Verify IP connectivity, SIP core/IMS configuration and proper routing and SIP signaling of a pre-arranged on demand Group Call		
Configuration(s)	- CFG_ONN_OTT-1 (5.2) - CFG_ONN_UNI-MC-LTE-1 (5.3) - CFG_ONN_MULTI-MC-LTE-1 (5.4)		
References	- SIP (see [n.4] and other references in [n.5]) - MCPT (see [n.6] and other references in [n.5]) - RTP (see [n.4] and other references in [n.5])		
Applicability	- MCPTT-Client_ONN-MCPTT-CALL, MCPTT-Client_AMR-WB, MCPTT-Client_AFFIL, MCPTT-Client_MCPTT-FC (6.2) - MCPTT-Part_ONN-MCPTT-CALL, MCPTT-Part_AFFIL (see NOTE), MCPTT-Part_MCPTT-FC, MCPTT-Part_RX (CFG_ONN_UNI-MC-LTE-1 only), MCPTT-Part_GCSE (CFG_ONN_MULTI-MC-LTE-1 only), (6.5) - MCPTT-Ctrl_ONN-MCPTT-CALL, MCPTT-Ctrl_AFFIL (see NOTE) (6.6)		
Pre-test conditions	- IP connectivity among all elements of the specific scenario - Proper configuration of the SIP core/IMS to forward the signaling to the specific controlling and participating servers - UEs properly registered to the SIP core/IMS and MCPTT system - Calling user is affiliated to the called group		
Test Sequence	**Step**	**Type**	**Description**
	1	stimulus	User 1 (mcptt_id_clientA@example.com) calls mcptt-group-A
	2	check	Dialog creating INVITE received at the MCPTT participating server of mcptt_id_clientA@example.com after traversing SIP core/IMS
	3	check	INVITE received at the MCPTT controlling server
	4	check	The MCPTT controlling server loads the affiliated members of the mcptt-group-A (either pre-configured or retrieved from the GMS) and creates an INVITE per each of the "n" members
	5	check	"n" INVITEs received at the MCPTT participating servers of each mcptt_id_clientX (where X:1..n)
	6	check	"n" INVITEs received at the affiliated mcptt_id_clientX
	7	check	"n" SIP dialogs established
	8	verify	Call connected and multiple media flows exchanged

Figure 6. Test Description example

3. MCX equipment providers jointly executed the different steps specified in the test description and evaluated interoperability through the different IOP Checks prescribed in the Test Description

   b. The MCX equipment provider recorded the Test Result in the Test Session Report, as follows:

      i. OK: all IOP Checks were successful

      ii. NOK: at least one IOP Check failed. A comment was requested.

      iii. NA: the feature was not supported by at least 1 of the involved EUTs. A comment was requested.

4. Once all the tests in the Test Session Report were executed and results recorded, the participants reviewed the Report and approved it.

8 Test Plan Overview

8.1 Introduction

This 3rd FRMCS Plugtests Test Plan was developed following ETSI guidelines for interoperability.

The Test Plan was reviewed and discussed with participants during the preparation and pre-testing phase. Considering the huge number of resulting test cases and difference expected maturity of the implementations and differences from participants in the previous Plugtests event and new companies, vendors selected the subset of test cases to evaluate in a per-testing slot basis.

New test cases implemented during the FRMCS Plugtests will become part of ETSI TS 103 564 after TCCE approval.

The following sections summarise the methodology used for identifying the different configuration and test objectives leading to different test cases subgroups.

8.2 Test configurations

The overall FRMCS ecosystem comprises both controlling and participating MCPTT/MCData/MCVideo application server(s) with integrated SIP core, FRMCS Clients, 5G access network with required PCC capabilities). Furthermore, a series of support servers were integrated in the so-called Common Services Core provide configuration, identity, group, and key management capabilities. Note, again 3GPP Release-17 compliant On-Network operations only were considered.

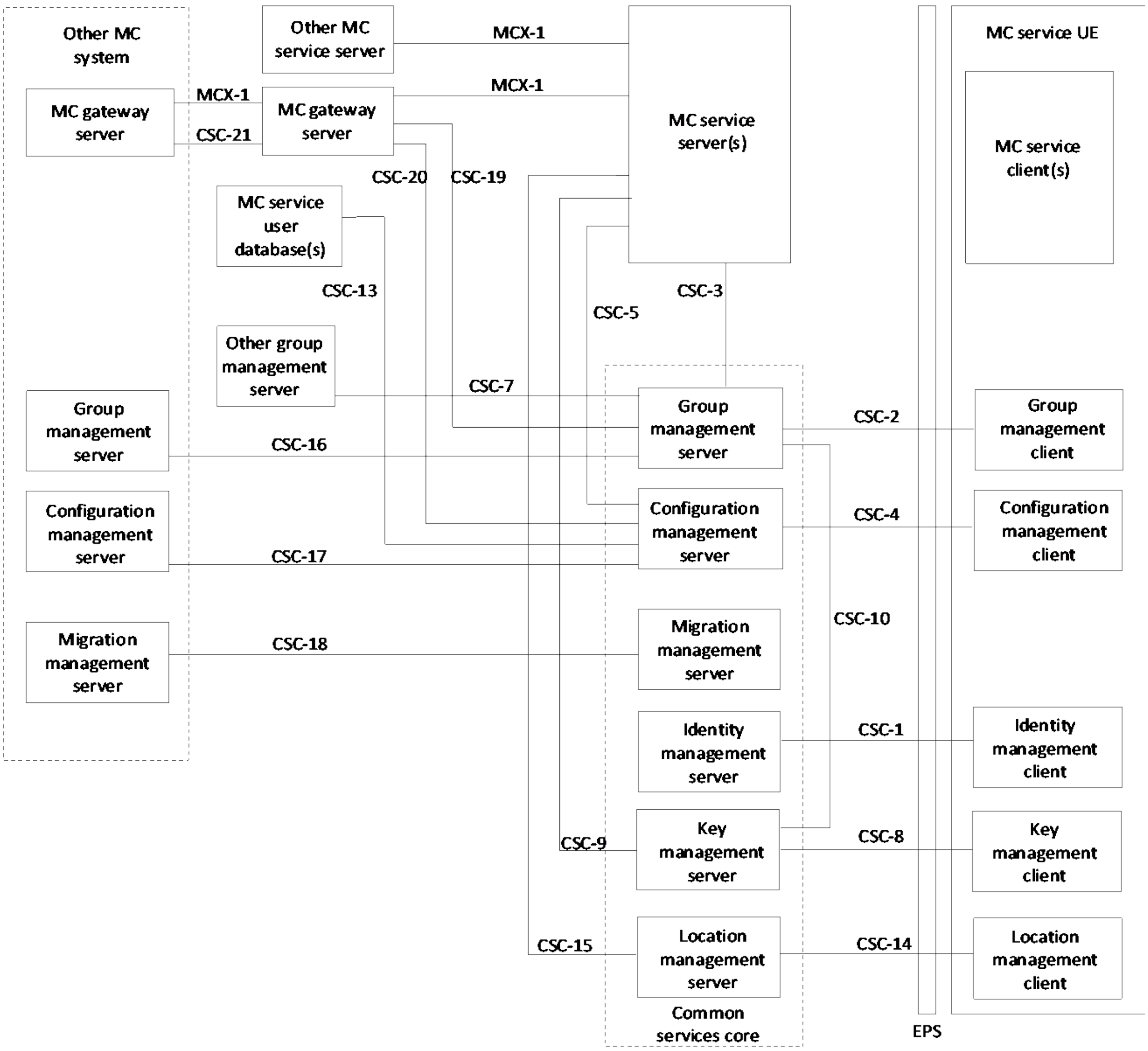


Figure 7. Functional model for application plane Figure 7.3.1-1 in 3GPP TS 23.280 [3].

Figure 7.3.1-1 in 3GPP TS 23.280 [3] describes the overall architecture and the reference points considered for the interoperability testing for any (MCPTT/MCData/MCVideo) MC Service (MCS). As can be seen, the resulting number of functional elements, interfaces and protocols involved is quite large. Furthermore, there are MCPTT/MCData/MCVideo-only specific interfaces and others (like N5/N33). In order to focus on MCS signalling the following three different configuration were initially considered: MCPTT/MCData/MCVideo as an application service over IP networks (Over-the-Top) and unicast Mission Critical 5G (all of them for On-Network calls only).

8.2.1 Over-The-Top Configuration for On-Network calls (CFG_ONN_OTT-1)

This configuration considered On-Network Calls (ONN) with a pure Over-The-Top (OTT) approach. It emulated a scenario where any underlying network (i.e. commercial 5G, WiFi or any wired technology such as Ethernet) would provide a bit-pipe type only access. No QoS/prioritization enforcement neither access-layer multi/broadcasting capabilities would be provided (i.e. nor unicast PCC support). Therefore, although not usable in a real world Mission Critical environment, it was used for connectivity tests since it did not require any binding between the IMS/SIP Core and the underlying 5G infrastructure and allowed both signalling and media plane parallel testing easily.

8.2.2 Unicast Mission Critical 5G for On-Network calls (CFG_ONN_UNI-MC -1)

In this configuration the 5G network (both 5GC and gNB) provided PCC capabilities and therefore enforced QoS policies in terms of prioritization and pre-emptiveness of Mission Critical unicast bearers. That included new Public Safety QCI 65/69 support in UEs and 5G Qi 65/69. Specific N5/MCPTT-5 reference points and unicast bearer setup and update triggering mechanisms were tested using this configuration. Note that, although MCPTT only is mentioned and depicted in the following figure, MCVideo/MCData could follow the same approach.

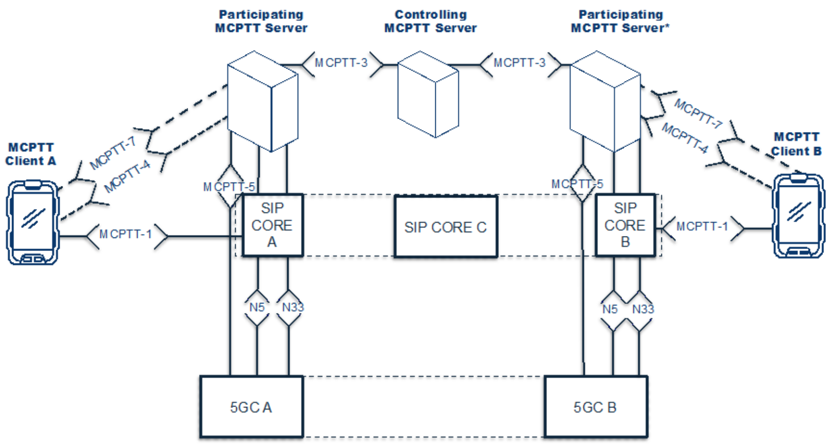


Figure 8. CFG_ONN_UNI-MC-LTE-1 configuration

In order to deal with the different test setting according to the three aforementioned configurations and cover specific more complex test configuration involving different clients and Observer test cases, the following configuration modes were defined in the TRT tool.

Configuration	Resulting configuration mode in the Plugtests (TRT)
ONN-OTT	PreTest-OTT-CabRadio PreTest-OTT-Client PreTest-OTT-Dispatcher
ONN-5G	FRMCS-IPConn FRMCS-RAN FRMCS-RAN-CabRadio FRMCS-RAN-Multi-AS FRMCS-RAN-Multi-Client

Table 10. Mapping of scenario architecture configurations and Plugtests event practical configurations

9 Interoperability Results

9.1 Overall Results

During the Plugtests event, a total of 85 Test Sessions were run: that is, 85 different combinations based on different configurations in Test Scope: FRMCS Client, FRMCS Server, gNB, 5GC, Dispatchers, UEs, CabRadios and Testers were tested for interoperability. Overall, 321 test executions were conducted and reported interoperability and conformance results.

The table below provides the overall results (aggregated data) from all the Test Cases run during all the Test Sessions with all the different combinations of Equipment Under Test from all the participating companies.

Among the executed Test Cases, the possible results were "OK", when interoperability was successfully achieved and "NO" (Not OK) when it was not.

Interoperability		Totals
PASS	FAIL	Run
276 (86.0%)	45 (14%)	321

Table 11. Overall Interoperability Results

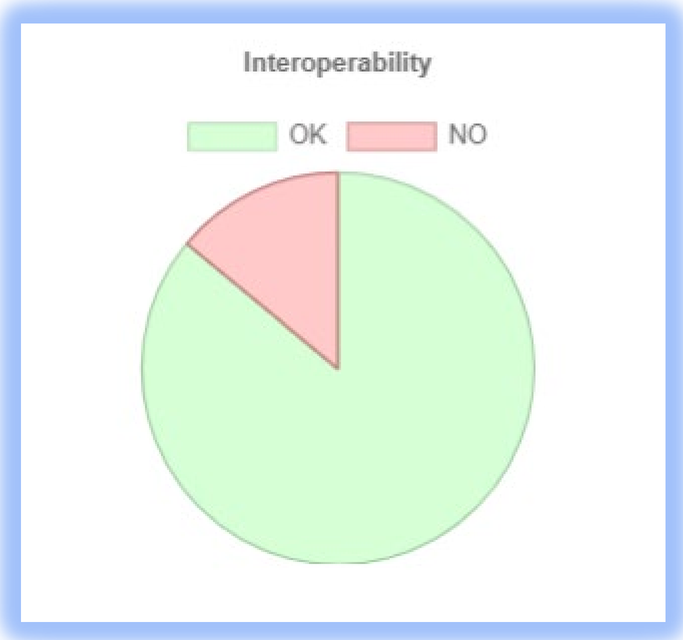


Figure 9. Overall Interoperability results (in %)

A overall interoperability success rate of 86% was achieved, which indicates a good degree of compatibility among the participating implementations (EUTs) in the areas of the Test Plan where features were widely supported and the test cases could be executed in most of the Test Sessions. In the next clauses, we will see that this high rate is also a consequence of the good preparation and involvement of participants during the remote integration and pre-testing phase of the Plugtests.

9.2 Results per Test Configuration

The table 18 below provides the results for each test configuration in the scope of the Plugtests event. The below configurations are defined in clause 7.2.

	Interoperability		
	OK	NO	Run
FRMCS-RAN	147 (88.0%)	20 (12.0%)	167
FRMCS-RAN-Multi-Client	12 (100.0%)	0 (0.0%)	12
FRMCS-RAN-Multi-AS	3 (100.0%)	0 (0.0%)	3
Conformance-Client	3 (75.0%)	1 (25.0%)	4
Conformance-AS	1 (100.0%)	0 (0.0%)	1
PreTest-OTT-Client	59 (74.7%)	20 (25.3%)	79
PreTest-OTT-Dispatcher	28 (93.3%)	2 (6.7%)	30
FRMCS-RAN-CabRadio	18 (90.0%)	2 (10.0%)	20
FRMCS-IPConn	1 (100.0%)	0 (0.0%)	1
PreTest-OTT-CabRadio	4 (100.0%)	0 (0.0%)	4

Table 12. Results per Test Configuration

The table shows that very high execution and interoperability rates for different Test Configurations were achieved.

9.3 Successful Integrations

The following figures 13 to 17 show the integrated equipments for each test stream. The grey lines show the initially planned integrations; the green lines show the successful pre-integrations; and the red lines show the actual integrations which were used for the tests during the Plugtests week.

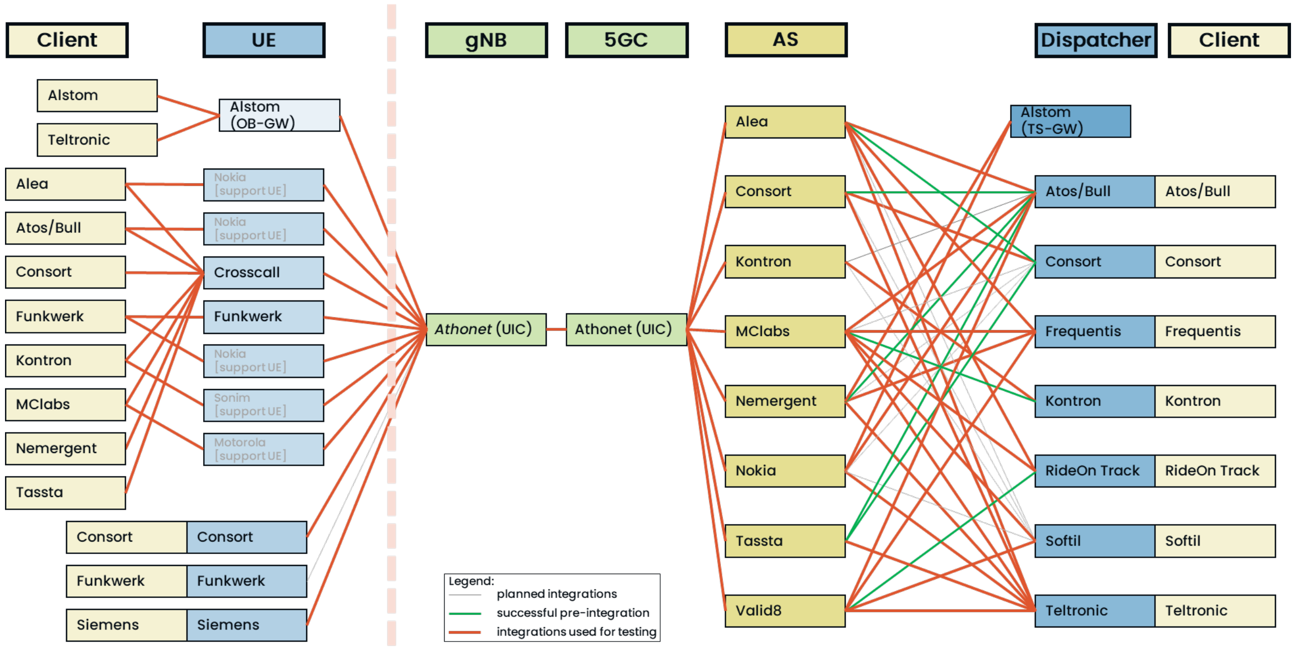


Figure 10. Available Equipment and integrations for Stream A: FRMCS over 5G

#

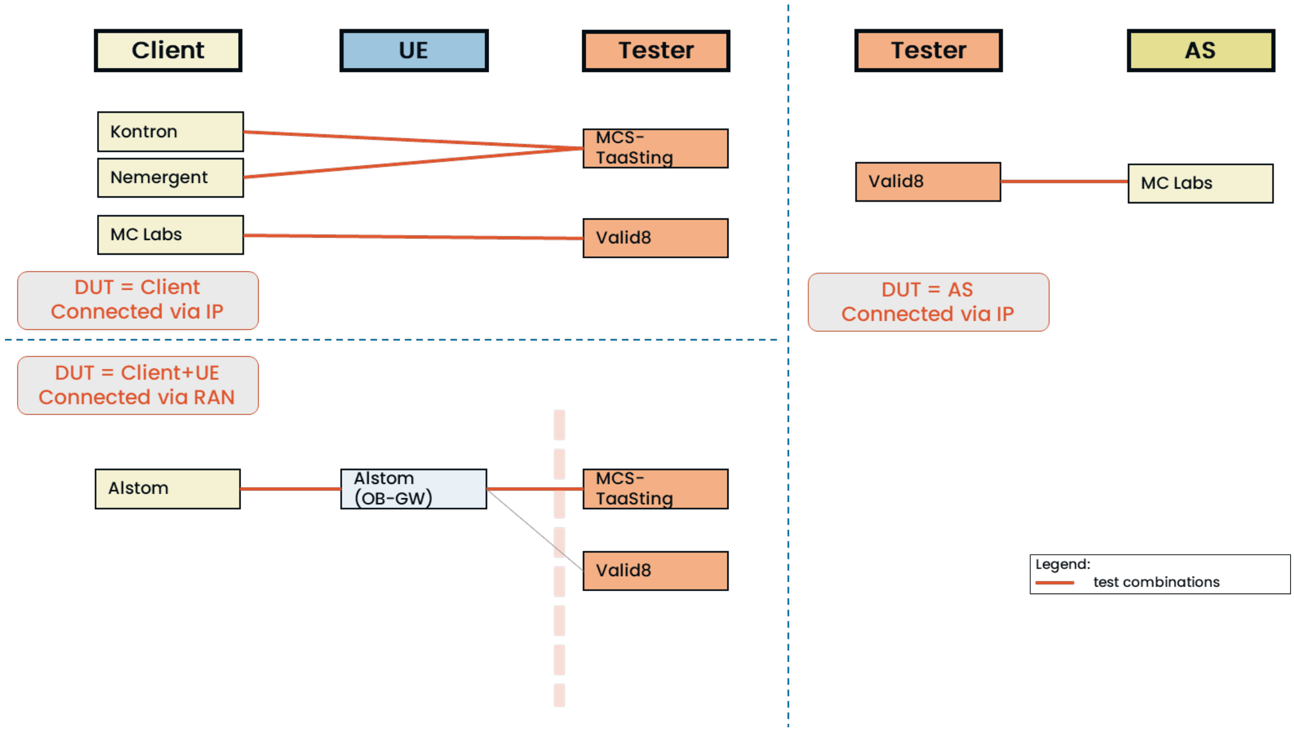


Figure 11. Available Equipment and integrations for Stream B: Conformance Testing

9.4 Results per Test Case

The table 19 below provides the results for each test case in the scope of the Plugtests event. Test Cases numbering is referred from ETSI TS 103 564 and attached test case document with the report.

Table 13. Results per Test Case

Interoperability			
Test Cases	**Pass**	**FAIL**	**Total**
7.2.5	3 (100.0%)	0 (0.0%)	3
7.2.15	31 (75.6%)	10 (24.4%)	41
7.2.16	25 (73.5%)	9 (26.5%)	34
7.2.17	1 (100.0%)	0 (0.0%)	1
7.2.18	0 (0.0%)	0 (0.0%)	0
7.2.23	2 (100.0%)	0 (0.0%)	2
7.2.25	0 (0.0%)	0 (0.0%)	0
7.2.29	7 (100.0%)	0 (0.0%)	7
7.2.38	0 (0.0%)	0 (0.0%)	0
7.2.40	0 (0.0%)	1 (100.0%)	1
7.2.41	0 (0.0%)	0 (0.0%)	0
7.2.43	0 (0.0%)	0 (0.0%)	0
7.2.44	0 (0.0%)	0 (0.0%)	0
7.2.49	5 (55.6%)	4 (44.4%)	9
7.2.50	5 (83.3%)	1 (16.7%)	6
7.2.62	0 (0.0%)	0 (0.0%)	0
7.2.67	5 (100.0%)	0 (0.0%)	5
7.2.68	5 (100.0%)	0 (0.0%)	5
7.2.73	0 (0.0%)	0 (0.0%)	0
7.2.120	4 (100.0%)	0 (0.0%)	4
7.2.121	0 (0.0%)	0 (0.0%)	0
7.2.128	0 (0.0%)	0 (0.0%)	0
7.2.129	0 (0.0%)	0 (0.0%)	0
7.2.130	0 (0.0%)	0 (0.0%)	0
7.2.131	0 (0.0%)	0 (0.0%)	0
7.2.132	0 (0.0%)	0 (0.0%)	0
7.4.1	22 (88.0%)	3 (12.0%)	25
7.4.3	27 (93.1%)	2 (6.9%)	29
7.5.9	1 (100.0%)	0 (0.0%)	1
7.5.10	2 (100.0%)	0 (0.0%)	2
7.5.15	0 (0.0%)	0 (0.0%)	0
7.5.16	0 (0.0%)	0 (0.0%)	0
7.9.10	2 (100.0%)	0 (0.0%)	2
7.9.11	0 (0.0%)	0 (0.0%)	0
7.12.1	0 (0.0%)	0 (0.0%)	0

7.12.2	0 (0.0%)	0 (0.0%)	0
7.13.1	32 (84.2%)	6 (15.8%)	38
7.13.2	26 (92.9%)	2 (7.1%)	28
7.13.3	7 (100.0%)	0 (0.0%)	7
7.13.4	7 (87.5%)	1 (12.5%)	8
7.13.5	8 (100.0%)	0 (0.0%)	8
7.13.6	8 (100.0%)	0 (0.0%)	8
7.13.7	26 (89.7%)	3 (10.3%)	29
7.13.8	3 (75.0%)	1 (25.0%)	4
7.13.9	0 (0.0%)	0 (0.0%)	0
7.13.10	2 (100.0%)	0 (0.0%)	2
7.15.1	1 (100.0%)	0 (0.0%)	1
7.15.2	1 (100.0%)	0 (0.0%)	1
7.15.3	1 (100.0%)	0 (0.0%)	1
7.15.4	1 (100.0%)	0 (0.0%)	1
9.14	0 (0.0%)	0 (0.0%)	0
10.5	1 (100.0%)	0 (0.0%)	1
10.6	0 (0.0%)	0 (0.0%)	0
10.7	0 (0.0%)	0 (0.0%)	0
10.8	0 (0.0%)	0 (0.0%)	0
10.9	0 (0.0%)	1 (100.0%)	1
10.10	0 (0.0%)	0 (0.0%)	0
10.11	1 (100.0%)	0 (0.0%)	1
10.12	0 (0.0%)	0 (0.0%)	0
Conformance	4 (80.0%)	1 (20.0%)	5

10 Plugtests Observations

As a result of the Plugtests event activities some issues in 3GPP Technical Specifications (TSs) and related standards were identified together with practical deployment problems that may demand some clarification or feedback from the related SDOs. We have classified those aspects into the following two categories:

- **Observations to MCX Standards**: Missing, erroneous or ambiguous definition of procedures in 3GPP's MCPTT TSs.
- **Technical constraints**: Related to implementation issues, not covered by the standards, but which need to be faced by MCX vendors in most deployments.

The reader should note that 3GPP Release 17 was considered for the third FRMCS Plugtests event.

The 3rd FRMCS Plugtests event team wants to thank all the participants in the Plugtests for kindly sharing the following lessons learned. Specific actions towards pushing this feedback to relevant TSGs in 3GPP have already been started at the time of the release of this report.

10.1 Observations

10.1.1 Encoding for the SDS payload for the text type

Section 15.2.13 in 3GPP TS 24.282 does not explicitly define the encoding for the text SDS payload.

In fact in stage 1 3GPP TS 22.282 ([R-5.2.2-004]) it is stated that "shall provide the option to include a content payload of at least [1000] characters of 8 bit text or [500] characters of 16 bit text or [250] characters of 32 bit text and the necessary character encoding information (for example to identify alphabet used)." That would mean that at least these 3 encoding should be supported and therefore signalling embedded somehow in the payload -automatic detection i.e. using BOM does not seem to be very interoperable and would not support the "necessary encoding information" sentence-.

10.1.2 Multiple GRE tunnels without GRE keys usage

In 3GPP TS 24.582, the usage of GRE-in-udp (RFC8086) is mandatory for a MCDATA-ipconn session; contrary to GRE-over-IP in the previous Rel. 16. Chapter 13.4 states that "GRE keys shall not be used". However, in some typical implementations such as GNU/Linux, GRE interface and UDP encapsulation are performed separately to result in GRE-in-udp encapsulation. As a result a Linux based device could have only one GRE interface with the same IP address and GRE key, for a same interface. This might be in line with the claim in RFC 8086 ("applications that rely on the GRE Key field for traffic separation or segregation"). So, if we try to mount a second GRE-in-udp tunnel with the same IP address for other application with no GRE key but different udp port, it will be seen as the same GRE tunnel on the GRE level and it is not possible to mount it.

10.1.3 Incoherence in the media description of IPconn session

There are an unclear description in chapter 13 of 3GPP TS 24.582 for media description to be put in a SIP INVITE for an IPconn session. In 13.5.2.1, there is this example:

```
m=application 20032 udp MCDATA
a=fmtp:MCDATA mcdata-ipconn
```

The second line is not coherent with chapter 13.6.2 describing the line "a=fmtp:[...]"

Additionally, the use of " is not clear in the description in chapter 13.6.2.1 Also the ABNF notation is not formally valid, because it mixes mcdata-ipconn-s-port (with a dash in s-port) and mcdata-ipconn-sport (with a dash in sport).

Moreover, the need of the fmtp line since the port number is unclear since it is already present in the media line.

10.1.4 Checksum in the IPconn media plane

This observation concerns the media plane of an IPconn session, which relies on GRE-in-udp (RFC8086) It is said in 13.4 of 3GPP TS 24.582:

```
1.)    UDP checksum shall be used when encapsulating in both IPv4 and IPv6;
```

However, it is not said whether the Checksum in the GRE layer shall or shall not be used. RFC 8086 states “Use of GRE checksum is RECOMMENDED when the UDP checksum is not used” and “The GRE checksum MAY be enabled to protect the GRE header and payload. When the UDP checksum is enabled, it protects the GRE payload, resulting in the GRE checksum being mostly redundant”. That would mean GRE checksum should not be present but a clarification would be nice to have for the vendors.

10.1.5 MCDATA-ipconn use of <mcdata-called-party-id>

This observation concerns the semantic regarding the signalling part of an IPconn session from Client A to Client B as described in Section D.1.3 in 3GPP TS 24.282. In the SIP INVITE sent by the participating terminating MCX AS to the target MCX client B, the <mcdata-info> contains some parameters which are sort of optional (e.g. the aforementioned TS states : "the <mcdata-called-party-id> can be included") It seems that the standard is not directive enough. Some clients expect the <mcdata-called-party-id> to have the id of the called party, some servers do not send it but use the <mcdata-request-uri> instead, to give the id of the called-party.

10.1.6 FA activation/deactivation

The procedures regarding functional alias activation defined in TS 24.379 are not fully clear to some vendors. In particular, clause 9A.2.1.2 states:

```
NOTE 3: Activation and deactivation of functional alias cannot be performed
with the same PUBLISH request.
6) shall include an application/pidf+xml MIME body indicating per-user
functional alias information according to clause 9A.3.1. In the MIME body,
the MCPTT client:
   a) shall include all functional aliases where the MCPTT user requests
activation for the MCPTT ID
```

However, in the beginning sof the very same clause it states “any combination of the above” including activation and deactivation and later in Clause 9A.2.2.2.3 Receiving functional alias status change from MCPTT client procedure contains the following steps state:

```
12)    if the candidate expiration interval is nonzero,   shall construct
the candidate list of the MCPTT functional alias entries as follows:
   a)   for each functional alias ID which has a functional alias information
entry in the served list of the functional alias information entries, such
that the expiration time of the functional alias information entry has not
expired yet, and which is indicated in a “functionalAliasID” attribute of a
<functionalAlias> element of the <status> element of the <tuple> element of
the <presence> root element of the application/pidf+xml MIME body of the SIP
PUBLISH request:
      i)      shall copy the functional alias information entry into a new
functional alias information entry of the candidate list of the functional
alias information entries;
      ii)      if the functional alias status of the functional alias
information entry is “deactivating” or “deactivated”, shall set the
functional alias status of the new functional alias information entry to the
“activated” state and shall set the activating p-id-fa of the new functional
alias information entry to the value of the <p-id-fa> element of the
<presence> root element of the application/pidf+xml MIME body of the SIP
PUBLISH request; and
      iii)     shall set the expiration time of the new functional alias
information entry to the current time increased with the candidate
expiration interval;
   b)   for each functional alias ID which has a functional alias information
entry in the served list of the functional alias information entries, such
```

```
that the expiration time of the functional alias information entry has not
expired yet, and which is not indicated in any "functionalAliasID" attribute
of the <functionalAlias> element of the <status> element of the <tuple>
element of the <presence> root element of the application/pidf+xml MIME body
of the SIP PUBLISH request:
      i)       shall copy the functional alias information entry into a new
functional alias information entry of the candidate list of the functional
alias information entries; and
      ii)      if the functional alias status of the functional alias
information entry is "activated" or "activating":
         -     shall set the functional alias status of the new functional
alias entry to the "deactivating" state; and
         -     shall set the expiration time of the new functional alias
information entry to the current time increased with twice the value of
timer F; and
   c)  for each functional alias ID:
      i)       which does not have a functional alias information entry in
the served list of the functional alias entries; or
      ii)      which has a functional alias information entry in the served
list of the functional alias information entries, such that the expiration
time of the functional alias information entry has already expired;
and which is indicated in a "functionalAliasID" attribute of the
<functionalAlias> element of the <status> element of the <tuple> element of
the <presence> root element of the application/pidf+xml MIME body of the SIP
PUBLISH request:
      i)       shall add a new functional alias information entry in the
candidate list of the functional alias information list for the functional
alias ID;
      ii)      shall set the functional alias status of the new functional
alias information entry to the "activating" state;
      iii)     shall set the expiration time of the new functional alias
information entry to the current time increased with the candidate
expiration interval; and
      iv)      shall set the activating p-id-fa of the new functional alias
information entry to the value of the <p-id-fa> element of the <presence>
root element of the application/pidf+xml MIME body of the SIP PUBLISH
request;
```

Comment on clause 9A.2.2.2.3: Bullet 12)

```
12)if the candidate expiration interval is nonzero, shall construct the
candidate list of the MCPTT functional alias entries as follows:
```

- Bullet a) basically means - "for each existing non-expired FA which has corresponding FA XML element in PIDF, we prolong expiration time and set to ACTIVATED status", meaning, it is for cases when FA in request is found in current served list

- Bullet b) basically means "deactivating currently active FAs which are not present in PIDF", meaning, it is for cases when there is some FA in current served list missing from the request which results in deactivation of that FA

- Bullet c) basically means "for each PIDF FA that has no existing (or has, but it is expired) FA entry we create new ACTIVATING FA", meaning, it is for cases when we create new FA which does not exist in current served list

The actions in bullet b could be a bit unexpected, where each "unmentioned" FAs in the request are deactivated , and later generate deactivation PUBLISH for these FAs.

Point 14) updates current list of FAs in PF storage with candidate list, and point 15) notices the differences between previous list of FAs and new ones and triggers potentially multiple SIP PUBLISH request towards CF

The problematic case is if the user has already functional aliases activated and wants to activate additional ones. According to clause 9A.2.2.2.3 it is necessary to send in the SIP PUBLISH request the already active functional aliases and the ones that are to be newly activated. If the already active functional aliases are not sent, they will be deactivated as stated in 9A.2.2.2.3 step 12)/b). In fact, the procedure in 9A.2.2.2.3: Bullet 12) allows activation and deactivation of functional aliases with one SIP PUBLISH request, while NOTE 3 in clause 9A.2.1.2 explicitly states that this is not possible.

10.1.7 Management of MCX clients behind gateway UE. NAT scenario

In FRMCS scenarios On-Board Cab Radios (MCX application clients) are installed behind one or several MC gateway UE in the same train which enables access to MCX server. MC gateways UE installed in the train aim to bring wireless connectivity not only to On-Board Cab Radios, but to many other applications in the train, not only one device. In addition, in a train there are usually at least two On-Board Cab Radios connected to the same MC gateway UE.

In the above-described scenario, several NAT related issues may appear due to possible overlaps or routing issues between the internal (behind the gateway UE) and MCX server one:

Issue 1: IP address

- SIP commands sent from MCX client (On-Board Cab Radio) towards MCX server are sent with:

o In IP layer: It is fulfilled with IP address of MCX gateway UE

o In SIP layer: It is fulfilled with IP address of On-Board Cab Radios behind MCX gateway UE

In the described scenario, MCX server receives SIP command, for example REGISTER command. However, the answer sent by server which destination is On Board Cab Radio is not reachable by MCX server because IP address of Cab Radio is out of its network. Only IP address of MCX gateway UE is reachable.

Issue 2: Communication ports

- On-Board cab radios use specific Signalling ports, Audio ports and MCPTT ports.

- Communication ports are usually dynamically changed and assigned on MC gateway UE being different to each device connected to this. In the described scenario, we meet again the same problem as described in Issue 1. RTP and RTCP traffic coming from MCX server cannot reach On-Board Cab radio, because the ports on On-Board cab radios and MC gateway UE will be different.

For these reasons and considering the NAT issues described above, the following possible solutions are ruled out : - Configuring Bridge mode in MC gateway UE is not a solution. - DHCP IP assignation method to configure in ETH interface in On-Board Cab Radios the same IP as that one configured in MC gateway UE.

Furthermore, some of the NAT traversal solution proposed are:

- Use of STUN to make the client aware of the NAT performed by the gateway, combined with NAT masquerading: However, there is no STUN server deployed in all customer projects. Neither in Plugtest.

- Use of a SIP proxy or SIP-ALG (or “MCX-proxy”) in the MC gateway UE: However not all MC gateway UE count of this facility.

- Enable IETF RFC 6263 to periodically send packet on the RTP/RTCP ports as defined in the SDP to keep the connection alive: However not all the servers have this solution. In addition, for those that count on this solution, they have implemented it with different methods, without following any standard.

Then a clarification regarding the usage (or forbidden usage) of NAT in such scenarios would be needed.

10.1.8 FA affiliation analogue to Group affiliation

According to TS 24.379, subclause 9A.2.1.2

4) if the MCPTT client requests to activate one or more functional aliases, shall set the Expires header field according to IETF RFC 3903 [37], to 4294967295; NOTE 2: 4294967295, which is equal to 232-1, is the highest value defined for Expires header field in IETF RFC 3261 [24].

5) if the MCPTT client requests to deactivate one or more functional aliases, shall set the Expires header field according to IETF RFC 3903 [37], to zero; and

NOTE 3: Activation and deactivation of functional alias cannot be performed with the same PUBLISH request.

This means that a PUBLISH needs to be sent to activate FAs, and an UNPUBLISH to deactivate them. Moreover, according to NOTE 3 a PUBLISH message can either activate or deactivate, but they cannot be mixed (e.g activate FA1 and deactivate FA2).

PAS/CAS sections have not been changed to work like that and they follow the same logic as affiliation procedures, where PUBLISHes are sent to affiliate/deaffiliate to/from groups (being able to mix both procedures in the same message) and an UNPUBLISH is sent to deaffiliate from all groups in just one message.

11 Observer Program

The Observers contributed to the FRMCS Plugtests in the definition of the scope and scenarios, in the Observer Program and for the Observer demo.

11.1 Preparation Phase

During equipment registration, interested vendors provided their intention to showcase during the observer demo. Test cases from ETSI TS 103 564 were used for the observer demo.

11.2 Observer Round Table Discussion

Observer round table discussions were organised on 04th July 2023 during FRMCS Plugtests event which focused on sharing of ideas, strategies, deployment challenges, conformance testing and performance of mission critical networks during the deployment. One of the major topics was "How does floor control signalling over QCI/5QI 69 improve MCS performance" by UK Home Office.

11.3 Observer Presentations

Observer programme is a presentation program during FRMCS Plugtests event which focused on the deployment plans and challenges of mission critical services.
The observer program provided a platform to the various stake holders in the critical communication industry to discuss the progress of FRMCS. The speakers were from government organisations, operators, regulators, users, associations which provide updates on deployment plans in their respective countries, pilot projects and updates on standards.

The observer program was conducted during half a day on 05th July 2023. The speakers presented to program outlined in Table 20.
Presentations in the observer program and the Questions & Answers are available on the Plugtests WIKI.

Presentations included:

Program	Name/Organisation	Allocated Time
Status of the Finnish Virve 2 program	Kari Juntilla / Erillisverkot	9:30 - 9:50
Update on TCCA Activities	Kevin Graham / TCCA	9:50 - 10:10
Conformance Task Force for Server to Server	Fidel Liberal / EHU	10:10 - 10:30
Coffee Break – 30 mins		
GCF TCCA Task Force on MCX Certification	Harald Ludwig / TCCA	11:00 – 11:30

FRMCS standardization status	Guillaume Gach / UIC	11:30 - 12:00
MCS networks work in mass events and key 5G features supported in roaming architecture based public safety networks	Nathan Jeyaratnarajah / UK Home Office	12:00 – 12:40

Table 14. Observer Program

11.4 Observer Demos

The Observer Demo was a possibility for vendors to present their solutions and features to the observers. The demos took place during the half day on 6th July 2023. The following demos were presented:

Demo no.	Time	Participants	Test Cases
#1	09:30 – 09:50	Softil, Valid8	ETSI TS 33.180, 5.1.1 Verifying Client limited-service state
#2	10:00 – 10:30	Alea, Athonet, Softil	10.2
#3	10:30 – 10:50	Nemergent, Athonet, Funkwerk, Crosscall, Frequentis	7.2.5, 7.2.15, 7.2.16, 7.2.49, 7.2.50, 7.13.1, 7.13.2, 7.15.1, 7.15.2, 7.15.3, 7.15.4
#4	11:00 – 11:20	Alstom, Nokia	7.4.1, 7.4.3, 7.2.120, 10.9

Table 15. Observer Demos

History

Document history		
V0.0.0	14/07/2023	First Draft
V0.2.0	28/07/2023	Draft with major changes
V0.3.0	02/08/2023	Stable Draft
V.0.4.0	10/08/2023	Stable Draft
V.0.5.0	22/08/2023	Stable Draft with corrections
V1.0.0	25/08/2023	Final report published