ETSI Plugtests Report V1.0.0 (2025-11)

5th ETSI FRMCS Plugtests
Paris, France
27 – 31 October 2025

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 fifth FRMCS Plugtests from 27th October to 31st October 2025 at the UIC Headquarter in Paris, France using 5G test networks. More than 300 test cases were executed between vendors, based on 3GPP Release-18.

The 5th ETSI FRMCX Plugtests have concluded with a success rate of 95% of the executed tests in the validation of FRMCS vendor interoperability. More than 180 delegates (100 onsite) participated during the 5th FRMCS Plugtests event.

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 fifth Plugtests started in June 2025, were followed by three weeks of integration with the test network and a one-week pre-testing in October 2025, and were finalized with a one week of face-to-face end-to-end interoperability testing with 5G test networks in October 2025 in Paris.

The tests were based on 3GPP Release-18 and more than 300 tests were executed between the different vendors in 96 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, Ad-hoc group call, IP Connectivity, GSM-R Interworking, Interconnection and Migration, etc.

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 5th FRMCS Plugtests was complemented by an observer program with presentations, round-table discussions and demos for the observers.

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

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

The next MCX Plugtests event is planned for June 2026. The next FRMCS Plugtests event is planned for November 2026.

The following observer organsiations participated in this Plugtests:

- Bane NOR, Norway
- BDBOS, Germany
- Erillisverkot, Public safety network operator, Finland
- French Ministry of Interior, France
- Home Office, United Kingdom
- MSB (Swedish Civil Contingencies Agency), Sweden
- Network Rail, UK
- Norwegian Directorate for Civil Protection, Norway
- ProRail, Netherlands
- SNCF Reseau, Railway Operator Research, France
- SNCF VOYAGEURS, Railway Operator Research, France
- Swiss Federal Railways Ltd (SBB AG), Switzerland
- TCCA, The Critical Communications Association
- Trafikverket, Sweden
- UIC Union Internationale des Chemins de Fer


Vendors
ETSI
ALEA
a LEONARDO company
ALSTOM
CROSSCALL
CYBERTEL bridge
Druid
EVIDEN
an atos business
CONSORT
funkwerk
HUAWEI
mclabs
Hytera
JIAXUN
FREQUENTIS
LEONARDO
nemergent
solutions
OCSTARS
kontron
RideOnTrack
STELE
Sanchar Telesystems Limited
SIEMENS
opale
systems
SED Wireless
SOFTIL
INNOVATIVE COMMUNICATIONS
Qualcomm
VALID8.com
TASSTA
Telematix
Smart telematic solutions
Teltronic


Observers
ETSI
astrid
adif
ALTA VELOCIDAD
BANE NOR
BDBOS
DSB
Erillisverkot
Home Office
MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité
MSB
SNCF
VOYAGEURS
NetworkRail
ProRail
SNCF
RÉSEAU
TCCA
SBB CFF FFS
TRAFIKVERKET
uic

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, ETSI and UIC, 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 5th ETSI FRMCS Plugtests event started in June 2025 with the registrations of vendors and observers. During bi-weekly conference calls from June to October 2025 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 5th 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 5th FRMCS Plugtests event wiki: https://wiki.plugtests.net/5th-FRMCS-Plugtests/index.php?title=Main_Page (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)
- GSM-R System

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 with multiple clients in same test sessions. Stream B was available for Interconnection and Migration testing and Stream D was available for GSM-R Interworking with FRMCS.

A dedicated Test Tools test stream (Stream C) 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 5th FRMCS Plugtests 18 additional test case scenarios were developed or/and updated by ETSI. In total, the FRMCS test specification has now more than 400 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. 95.5 % of the tests were successful, the remaining 4.5 % 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#6 Plugtests session is planned for Q4 2026. 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 18 versions for the fourth FRMCS 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
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 (Figure 1) illustrates the basic test infrastructure.

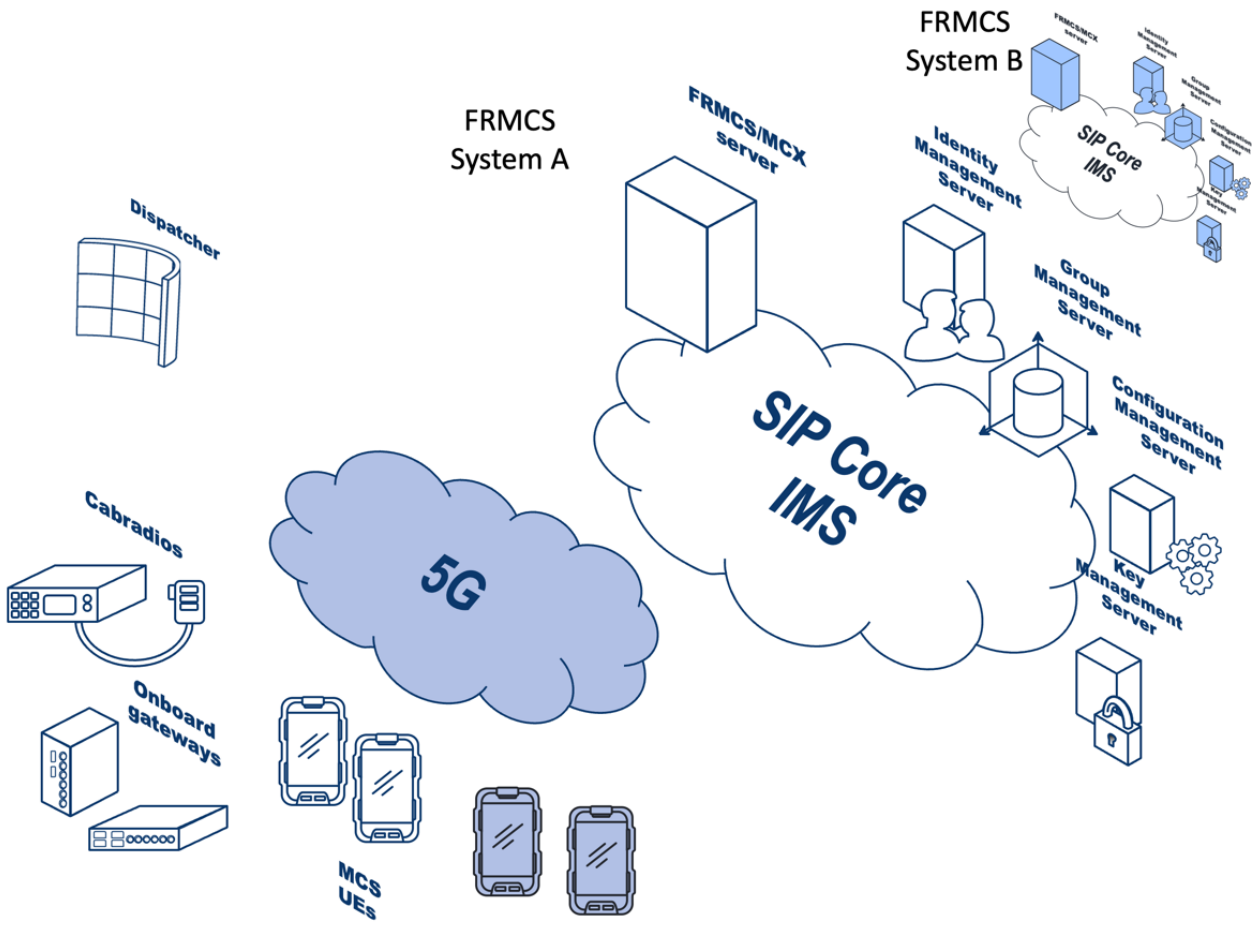

Figure 1. Typical MCPTT/MCData/MCVideo scenario to be considered in the Plugtests

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. 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. Application level refers to e2e signalling, media, floor controlling (and other involved) protocols in use.

- **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.

- **GSM-R Interworking Scenarios:** Comprised FRMCS and GSM-R interworking.
- **Affiliation (AFFIL)**: Comprises MCX Client explicit and implicite affiliation
- **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.
- **Interconnection and Migration Scenarios:** Comprised Interconnection and Migration of different group calls.
- **Adhoc Group Call** - Group call test cases for a temporary and dynamic communication setup within mission-critical services.

4.2 Timeline

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

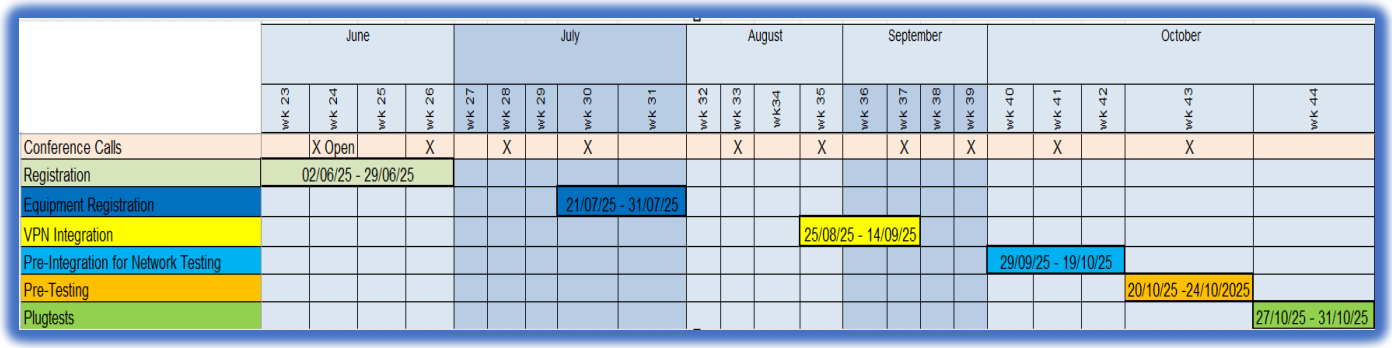

Figure 2. Plugtests event timeline

Registration to the FRMCS Plugtests event was open from 02 June 2025 to 29 June 2025 to any organisation willing to participate in testing the FRMCS Ecosystem. A total of 185 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-18 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 25th August to 14th September 2025, participants connected their equipment's with ETSI HIVE infrastructure to collaboratively run the pretesting remotely.

From 29th September to 19th October 2025, participants connected their equipment's with 5G networks to collaboratively run the Interoperability Test Sessions remotely. Over the top IP based testing was performed by during the pretesting phase from 20th October to 24th October 2025.

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, B and D.

During this phase, up to 26 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 27th October to 31st October 2025 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.
- **Registration** – Information about the registration.
- **RoE and NDA** – Rules of Engagement and NDA
- **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.
- **Conf Calls** - Calendar, logistics, agendas and minutes of the bi-weekly conference calls run during the remote integration and pre-testing phase.

- **Observer Program & Demo** – 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.
- **Observations** - Issues found during Plugtests event.
- **Host Information** – Information about the host facilities.
- **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
Consort Digital	MCPTT, MCDATA
Cybertel	MCPTT, MCDATA
Eviden	MCPTT, MCDATA
Frequentis	MCPTT, MCDATA
Hytera	MCPTT, MCDATA
Jiaxun	MCPTT, MCDATA
Kontron	MCPTT, MCDATA
MCLabs	MCPTT, MCDATA
Nemergent	MCPTT, MCDATA
Pocstars	MCPTT, MCDATA
Shenzhen SED	MCPTT, MCDATA
Tassta	MCPTT, MCDATA
Teltronic	MCPTT, MCDATA
Valid8	MCPTT, MCDATA

Table 1. FRMCS/MCX Application Servers Under Test

5.2 FRMCS/MCX Clients

Organisation	Support
Alea	MCPTT, MCDATA
Consort Digital	MCPTT, MCDATA
Cybertel	MCPTT, MCDATA
Eviden	MCPTT, MCDATA
Funkwerk	MCPTT, MCDATA
Hytera	MCPTT, MCDATA
Jiaxun	MCPTT, MCDATA
Kontron	MCPTT, MCDATA
Nemergent	MCPTT, MCDATA
Pocstars	MCPTT, MCDATA
Sanchar	MCPTT
Shenzhen SED	MCPTT, MCDATA
Softil	MCPTT, MCDATA
Teltronic	MCPTT, MCDATA

Table 2. FRMCS/MCX Clients Under Test

5.3 Dispatcher (DISP)

Organisation	Support
Frequentis	MCPTT, MCDATA
Hytera	MCPTT, MCDATA
Jiaxun	MCPTT, MCDATA
RideOnTrack	MCPTT, MCDATA

Organisation	Support
Softil	MCPTT, MCDATA
Teltronic	MCPTT, MCDATA
Valid8	MCPTT, MCDATA

Table 3. Dispatcher (DISP) Under Test

5.4 5G Systems Core (5GC) + gNB (5G New Radio)

Organisation	Support
Druid	
Huawei	
Kontron	
Teltronic	
Valid8	

Table 4. 5G Systems Under Test

5

5.5 User Equipment (UE)

Organisation	Support
Alstom	On-board Gateway, Track-side Gateway
Consort Digital	Cab radio
Crosscall	5G Device
Cybertel	5G Device
Funkwerk	5G Device, Cab radio
Hytera	5G Device, Cab radio
Leonardo	Cab radio
Qualcomm	On-board Gateway
Shenzhen SED	5G Device, On-board Gateway, Track-side Gateway
Siemens	Cab radio
Teltronic	Cab radio
Tianjin 712 Mobile	Cab radio, On-board Gateway

Table 6. User Equipment Under Test

5.6 Test Tools

Organisation	Support
Opale	KPI Tester
Valid8	MCX Conformance Tester

Table 7. Testers Under Test

5.7 GSM-R System

Organisation	Support
Kontron	GSM-R

Table 8. GSM-R 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 3:

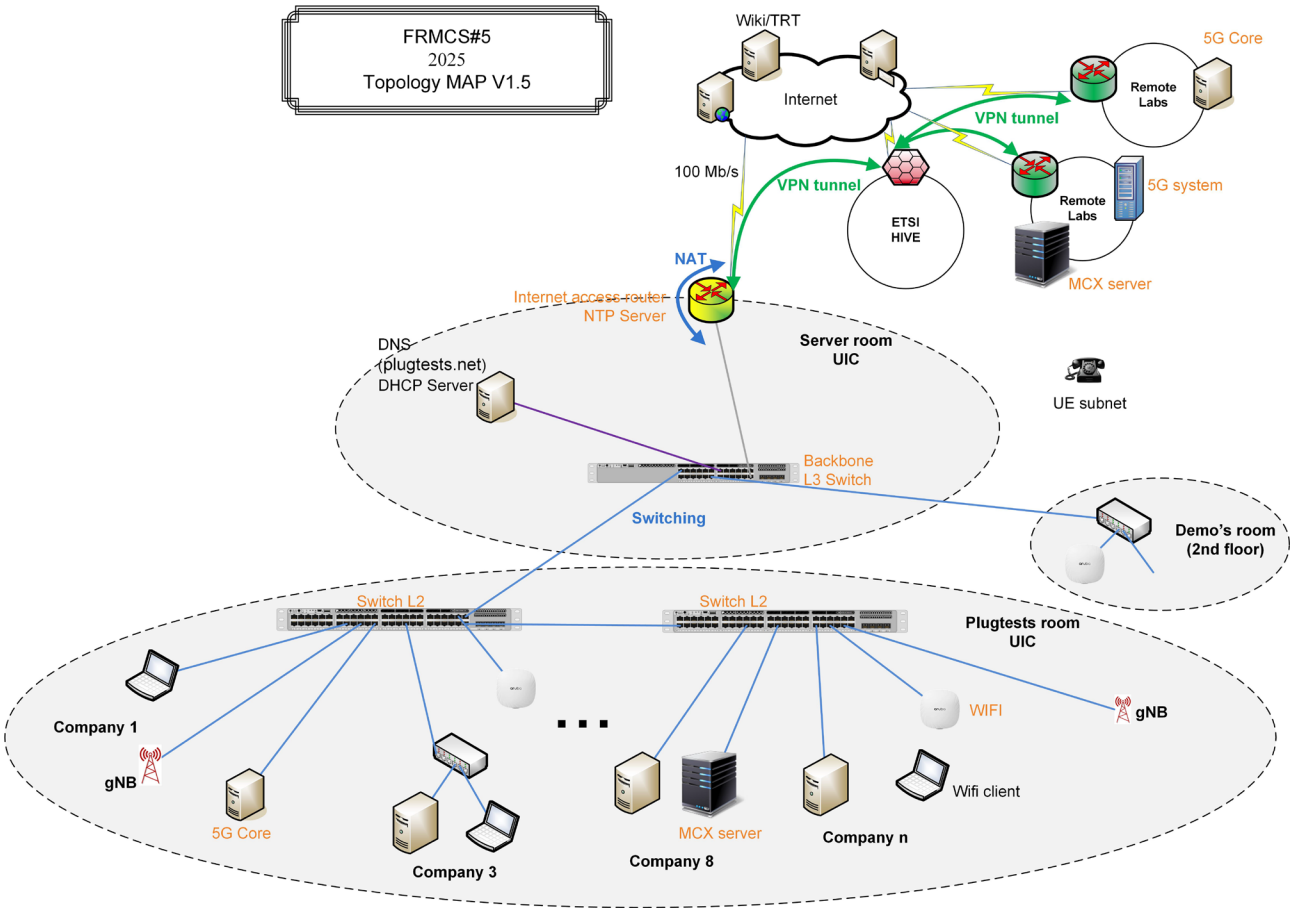

Figure 3. Remote Test Infrastructure

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 26 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
Config-Pretest- OTT	MCX Client + MCX AS
Config-Pretest-OTT-Cabradio	Cabradio + MCX AS
Config-Pretest-OTT-Disp	MCX AS + Dispatcher
Config-Pretest-InterMCX	MCX Client + MCX AS + MCX Client + MCX AS
Config-Integration-AS	5GS + MCX AS

Table 9. 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
Config-FRMCS	MCX Client + MCX AS + MCX Client + 5GS
Config-FRMCS-Disp	Dispatcher + MCX Client + MCX AS + MCX Client + 5GS
Config-FRMCS-Cabradio	Cabradio + MCX Client + MCX AS + 5GS
Config-FRMCS-Cabradio-Disp	Dispatcher + Cabradio + MCX Client + MCX AS + 5GS
Config-FRMCS-Cabradios	Cabradio + Cabradio + MCX AS + 5GS
Config-FRMCS-Cabradios-Disp	Dispatcher + Cabradio + Cabradio + MCX AS + 5GS
Config-FRMCS-OB-TSGW	OB GW + MCX Client + MCX AS + 5GS
Config-InterMCX	MCX Client + MCX AS + MCX Client + MCX AS + 5GS
Config-InterMCX-Disp	Dispatcher + MCX Client + MCX AS + MCX Client + MCX AS + 5GS
Config-IWF-GSMR	GSM-R + MCX Client + MCX AS + 5GS
Config-Tester-AS	Tester + MCX AS
Config-Tester-Client	Tester + MCX Client

Table 10. 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.

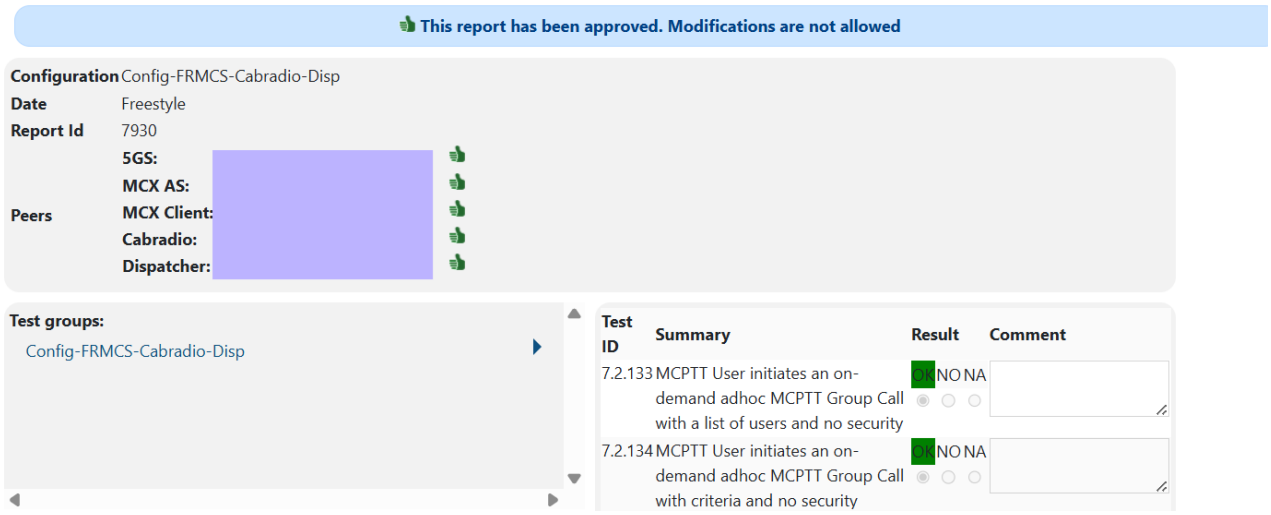

Figure 4. Test Session Report

2. For each Test in the Test Plan:

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

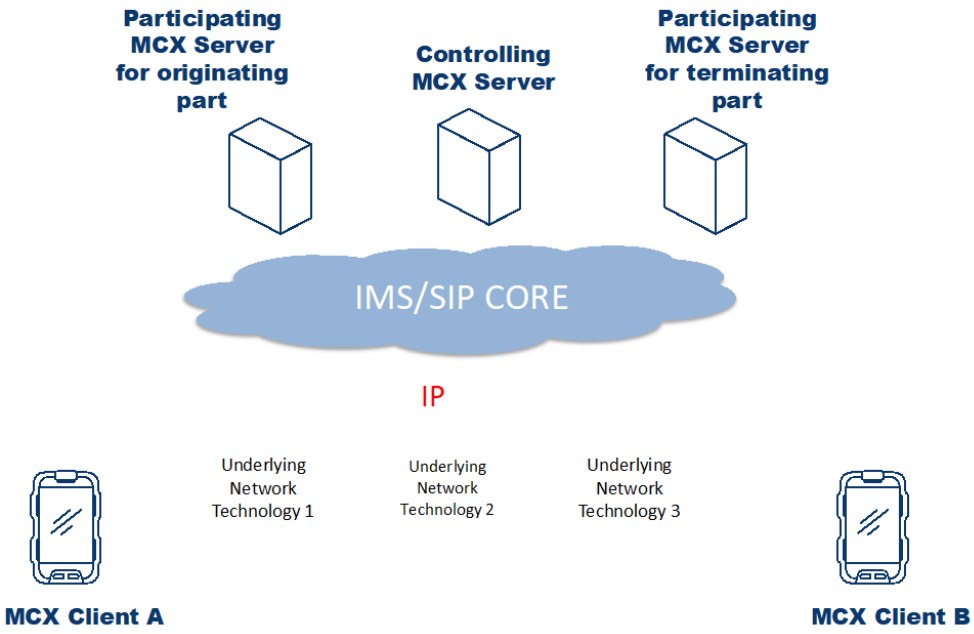

Figure 5. System Under Test (SUT) Configuration – MCX example

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 preconfigured 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 5th 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 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-18 compliant On-Network operations only were considered.

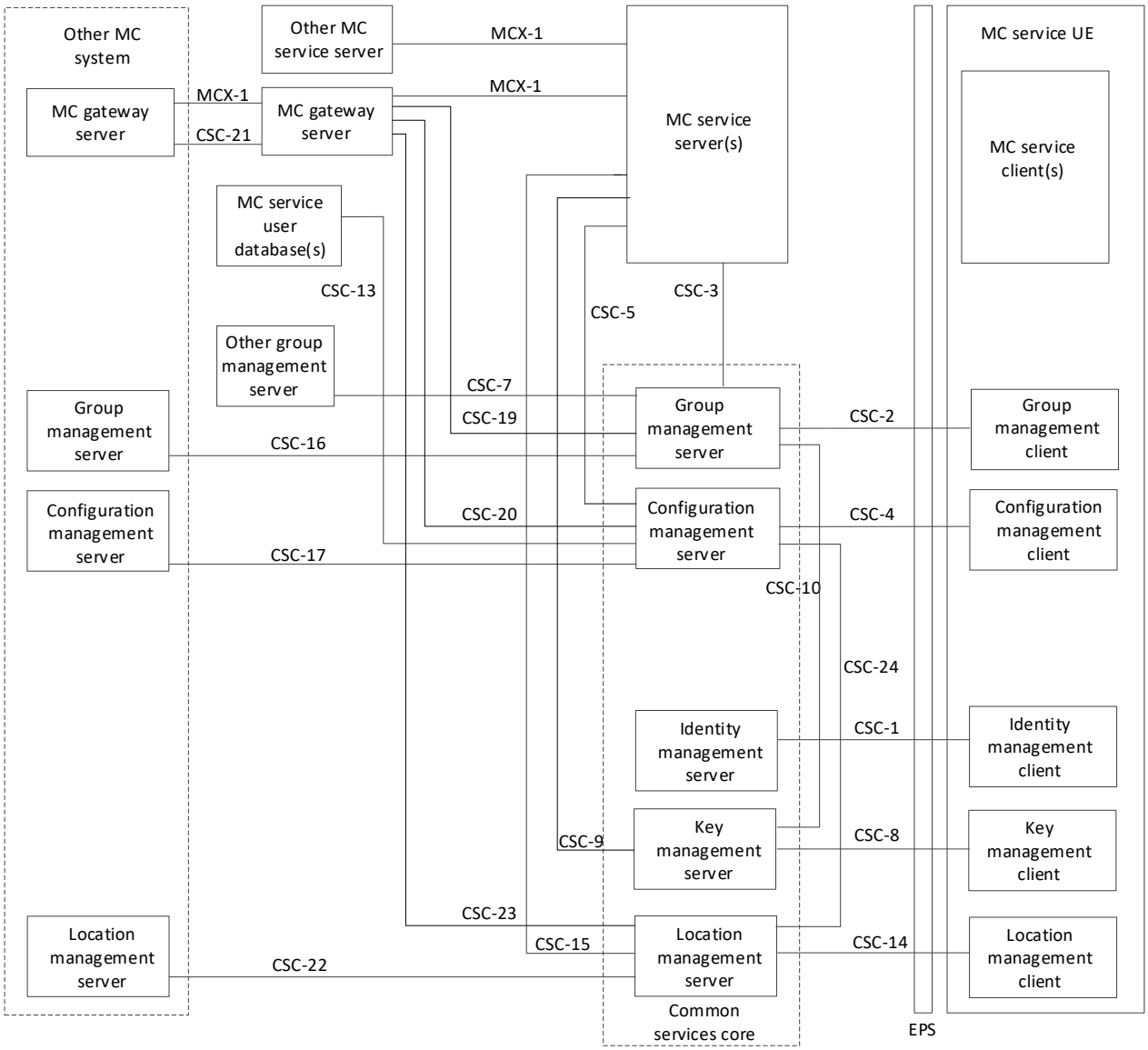

Figure 7. Functional model for application plane Figure 7.3.1-1 in 3GPP TS 23.280 [3].

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) 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 -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 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 Mission Critical 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 8, MCVideo/MCData could follow the same approach.

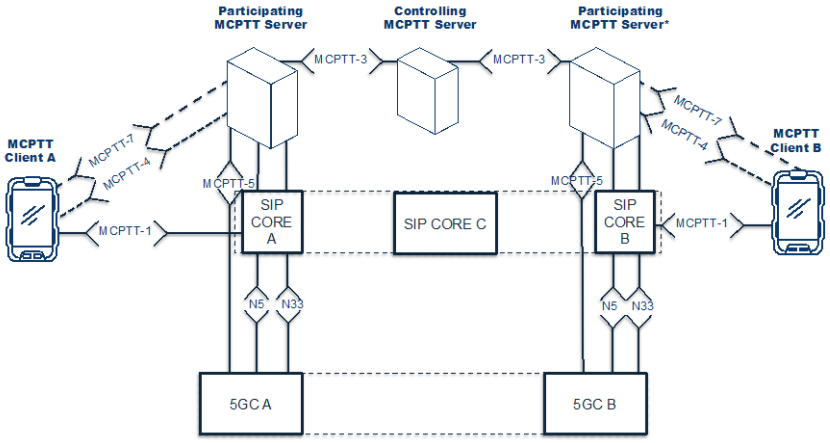

Figure 8. CFG_ONN_UNI-MC-1 configuration

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	Config-Pretest- OTT Config-Pretest-OTT-Cabradio Config-Pretest-OTT-Disp Config-Pretest-InterMCX Config-Integration-AS
ONN-5G	Config-FRMCS Config-FRMCS-Disp Config-FRMCS-Cabradio Config-FRMCS-Cabradio-Disp Config-FRMCS-Cabradios Config-FRMCS-Cabradios-Disp Config-FRMCS-OB-TSGW Config-InterMCX Config-InterMCX-Disp Config-IWF-GSMR Config-Tester-AS Config-Tester-Client

Table 11. Mapping of scenario architecture configurations and Plugtests event practical configurations

9 Interoperability Results

9.1 Overall Results

During the Plugtests event, a total of 95 Test Sessions were run: that is, 95 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, 332 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**
316 (95.5 %)	15 (4.5 %)	331

Table 12: Overall Interoperability Results

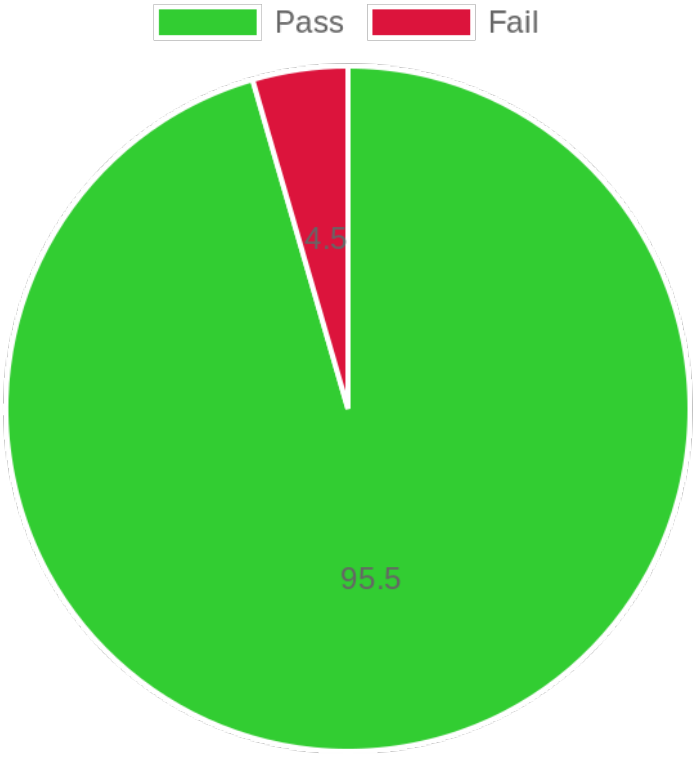

Figure 9. Overall Interoperability results (in %)

A overall interoperability success rate of 95.5 % 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 13 below provides the results for each test configuration in the scope of the Plugtests event. The below configurations are defined in clause 7.2.

Configurations	Pass	Fail	Total
Config-FRMCS-Disp	60 (90.3%)	7 (9.7%)	72
Config-FRMCS	89 (98.9%)	1 (1.1%)	90
Config-FRMCS-Cabradio	75 (93.8%)	5 (6.3%)	80
Config-InterMCX	2 (100.0%)	0 (0.0%)	2
Config-InterMCX-Disp	0 (0.0%)	0 (0.0%)	0
Config-IWF-GSMR	0 (0.0%)	1 (100.0%)	1
Config-FRMCS-Cabradios	12 (100.0%)	0 (0.0%)	12
Config-FRMCS-Cabradio-Disp	51 (100.0%)	0 (0.0%)	51
Config-FRMCS-Cabradios-Disp	13 (100.0%)	0 (0.0%)	13
Config-FRMCS-OB-TSGW	9 (90.0%)	1 (10.0%)	10

Table 13. 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 Figure 10 and Figure 13 show the integrated equipments for each test stream. The grey lines show the initially planned integrations; the blue lines show the successful pre-integrations; and the green lines show the integrations which were used for the interoperability testing during the Plugtests week. Please note that over-the-top tests are not shown in the diagrams.

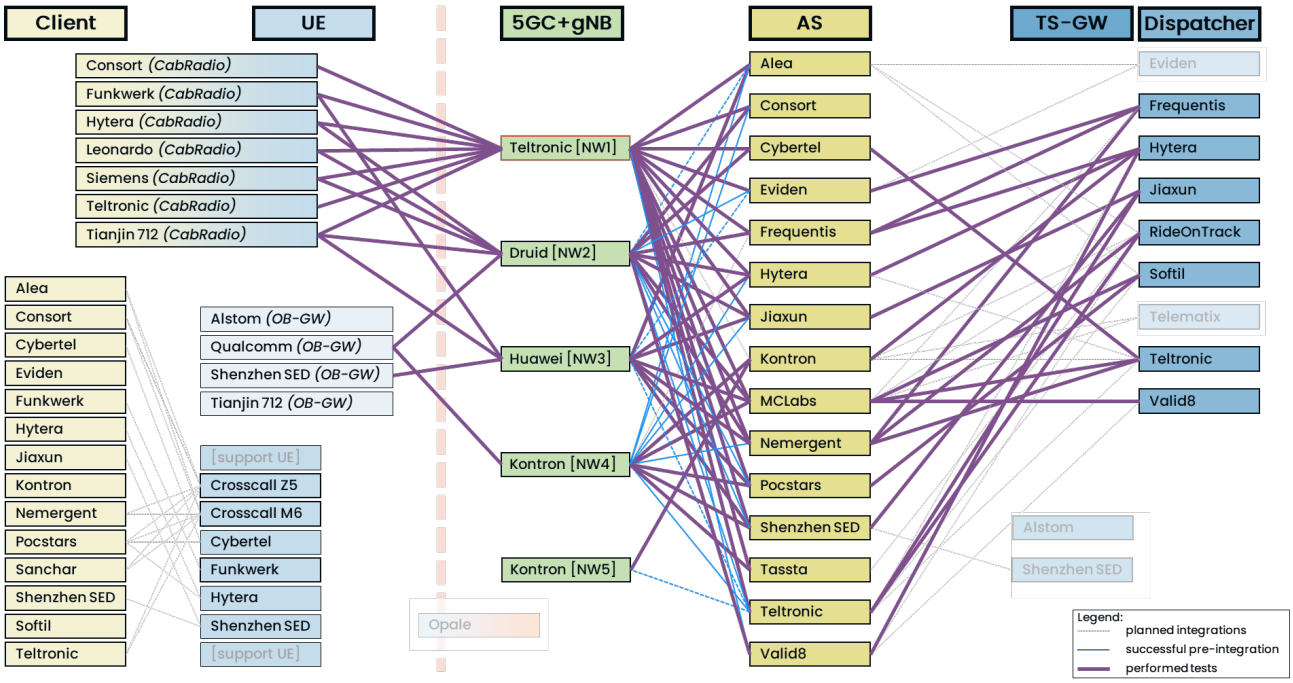

Figure 10. Available Equipment and integrations for Stream A: FRMCS over 5G

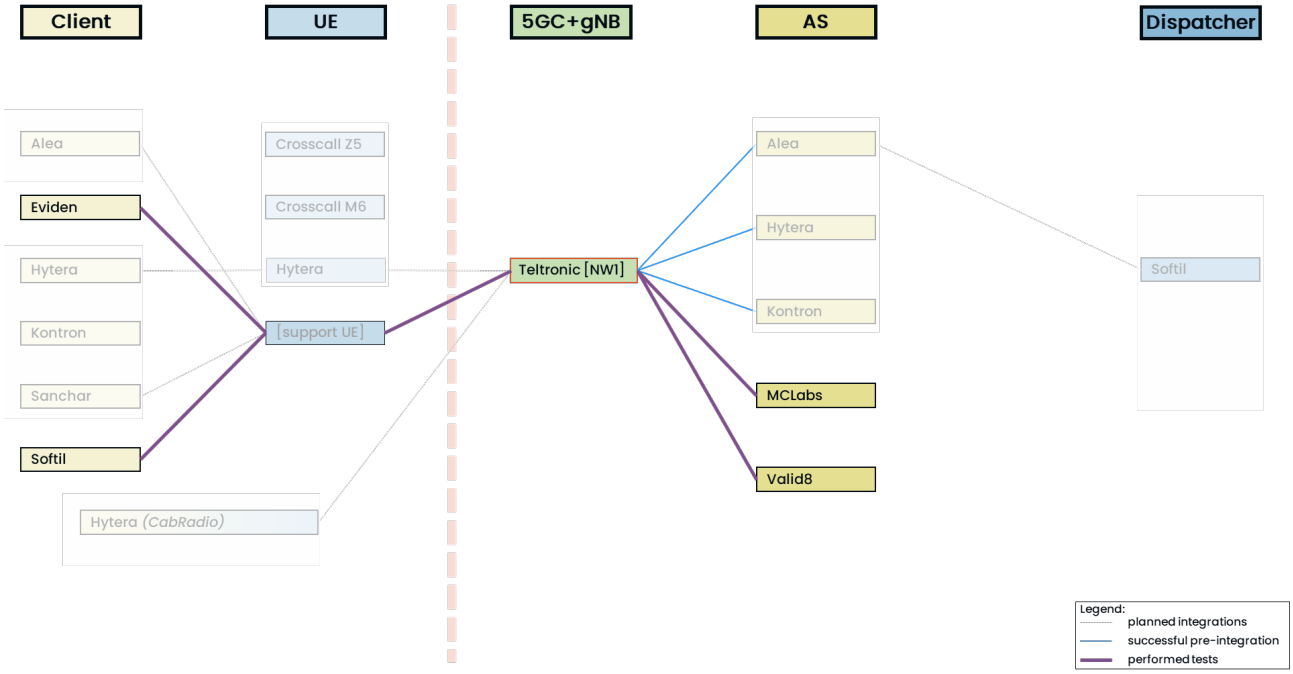

Figure 11. Available Equipment and integrations for Stream B: Interconnect and Migration

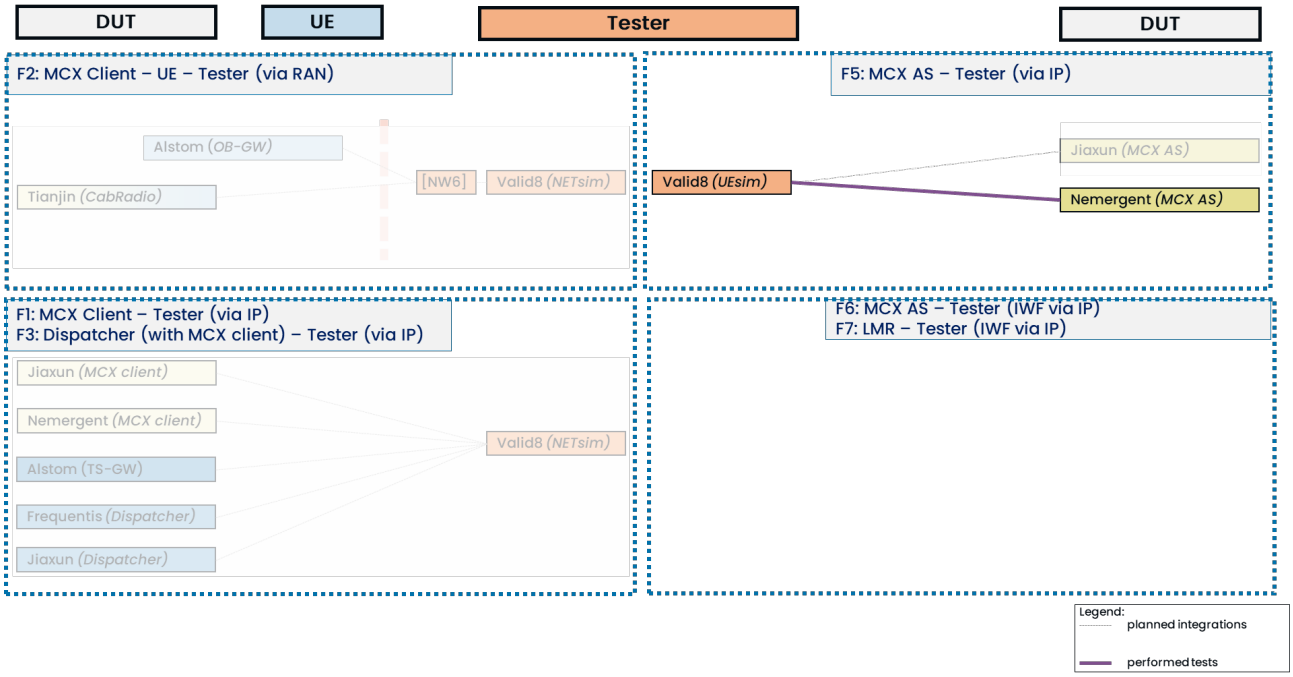

Figure 12. Available Equipment and integrations for Stream C: Conformance Testing

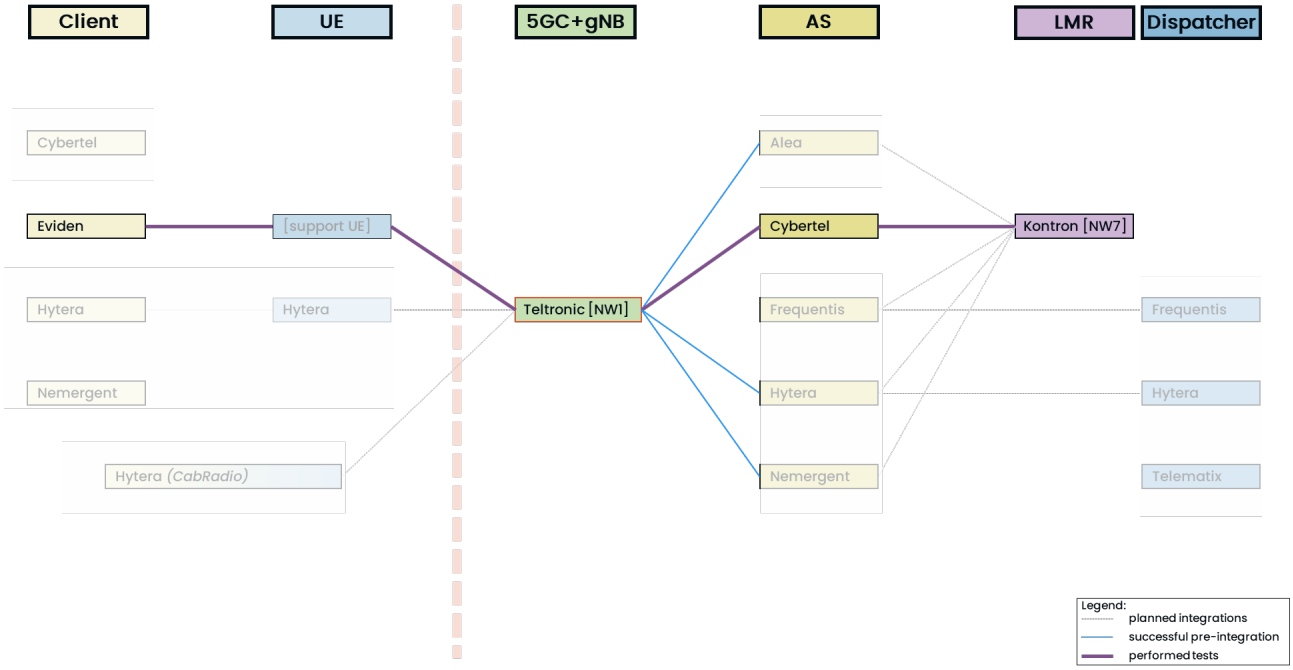

Figure 13. Available Equipment and integrations for Stream D: Interworking Function

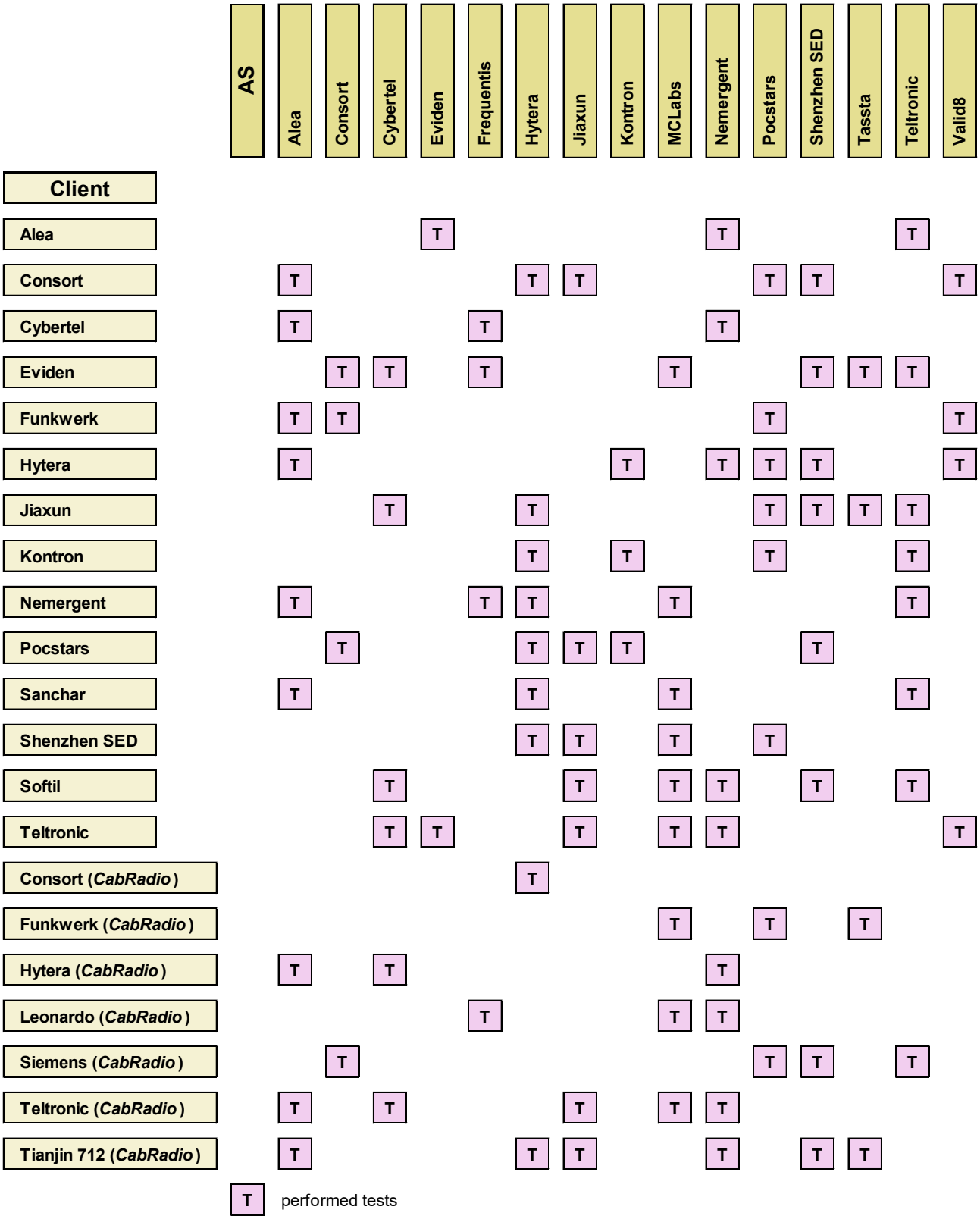

Figure 14. Tested Client-Server Relations over all Streams

9.4 Results per Test Case

The table 14 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.

Test Case	Pass	Fail	Results
7.2.133	55 (87.3%)	8 (12.7%)	63
7.2.134	22 (95.7%)	1 (4.3%)	23
7.2.135	3 (100.0%)	0 (0.0%)	3
7.2.136	1 (100.0%)	0 (0.0%)	1
7.2.137	53 (98.1%)	1 (1.9%)	54
7.2.142	0 (0.0%)	0 (0.0%)	0
7.2.149	0 (0.0%)	0 (0.0%)	0
7.2.150	0 (0.0%)	0 (0.0%)	0
7.2.151	1 (100.0%)	0 (0.0%)	1
7.2.152	0 (0.0%)	0 (0.0%)	0
7.2.153	1 (100.0%)	0 (0.0%)	1
7.2.154	1 (100.0%)	0 (0.0%)	1
7.2.155	0 (0.0%)	0 (0.0%)	0
7.3.2	28 (96.6%)	1 (3.4%)	29
7.3.3	25 (96.2%)	1 (3.8%)	26
7.3.4	9 (100.0%)	0 (0.0%)	9
7.3.5	7 (100.0%)	0 (0.0%)	7
7.3.6	5 (100.0%)	0 (0.0%)	5
7.3.7	4 (80.0%)	1 (20.0%)	5
7.3.8	5 (83.3%)	1 (16.7%)	6
7.3.9	3 (100.0%)	0 (0.0%)	3
7.4.6	0 (0.0%)	0 (0.0%)	0
7.4.7	1 (100.0%)	0 (0.0%)	1
7.4.8	0 (0.0%)	0 (0.0%)	0
7.4.9	0 (0.0%)	0 (0.0%)	0
7.5.7	0 (0.0%)	0 (0.0%)	0

7.5.8	1 (100.0%)	0 (0.0%)	1
7.5.9	20 (100.0%)	0 (0.0%)	20
7.5.10	47 (100.0%)	0 (0.0%)	47
7.5.11	0 (0.0%)	0 (0.0%)	0
7.5.12	0 (0.0%)	0 (0.0%)	0
7.5.13	0 (0.0%)	0 (0.0%)	0
7.5.14	1 (100.0%)	0 (0.0%)	1
7.5.15	5 (100.0%)	0 (0.0%)	5
7.5.16	9 (100.0%)	0 (0.0%)	9
7.5.17	0 (0.0%)	0 (0.0%)	0
7.5.18	0 (0.0%)	0 (0.0%)	0
7.9.10	1 (100.0%)	0 (0.0%)	1
7.9.11	0 (0.0%)	0 (0.0%)	0
7.14.18	0 (0.0%)	0 (0.0%)	0
7.14.19	0 (0.0%)	0 (0.0%)	0
9.14	0 (0.0%)	0 (0.0%)	0
10.5	0 (0.0%)	0 (0.0%)	0
10.9	1 (100.0%)	0 (0.0%)	1
10.10	1 (100.0%)	0 (0.0%)	1
10.11	1 (100.0%)	0 (0.0%)	1
10.12	2 (100.0%)	0 (0.0%)	2
11.3.1	0 (0.0%)	0 (0.0%)	0
11.3.4	0 (0.0%)	0 (0.0%)	0
11.3.5	0 (0.0%)	0 (0.0%)	0
11.3.6	0 (0.0%)	0 (0.0%)	0
11.3.7	0 (0.0%)	0 (0.0%)	0
11.3.8	0 (0.0%)	0 (0.0%)	0

11.3.9	0 (0.0%)	0 (0.0%)	0
11.3.10	0 (0.0%)	0 (0.0%)	0
11.3.11	0 (0.0%)	0 (0.0%)	0
11.3.12	0 (0.0%)	0 (0.0%)	0
11.3.13	0 (0.0%)	1 (100.0%)	1
11.3.14	0 (0.0%)	0 (0.0%)	0
11.3.15	0 (0.0%)	0 (0.0%)	0
11.3.16	0 (0.0%)	0 (0.0%)	0
11.3.19	0 (0.0%)	0 (0.0%)	0
11.3.20	0 (0.0%)	0 (0.0%)	0
11.3.21	0 (0.0%)	0 (0.0%)	0
11.3.22	0 (0.0%)	0 (0.0%)	0
11.3.23	0 (0.0%)	0 (0.0%)	0
11.3.24	0 (0.0%)	0 (0.0%)	0
11.3.25	0 (0.0%)	0 (0.0%)	0
11.3.26	0 (0.0%)	0 (0.0%)	0
11.3.27	0 (0.0%)	0 (0.0%)	0
11.3.28	0 (0.0%)	0 (0.0%)	0
10.13	1 (100.0%)	0 (0.0%)	1
10.3	3 (100.0%)	0 (0.0%)	3

Table 14. Results per Test Case

10 Plugtests Observations to the FRMCS/MCX Standards

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 FRMCS/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 18 was considered for the fifth FRMCS Plugtests event.

The 5th 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 to FRMCS/MCX Standards

10.1.1 Lack of integrity/confidentiality protection in partner system for the migration deauthorized notification

Test case 7.4.7 shows how the client in the partner system is capable of protecting the mcptt-id associated elements in the migration authorization request (that would be therefore hidden in the SIP/IMS Core of the partner system). However, there is no sibling behaviour for the primary system sending the deauthorizated notification, since the SIP message (that could be in the clear in the path from the primary to the partner system) is simply forwarded between the participating and the migrated Client.

10.1.2 Late call entry and partner/primary affiliation depending on where the group is hosted

Clause 10.16.2 in 3GPP TS 23.280 depicts a situation for late call entry when migrating but whether the "service continuity" like behaviour demands the user before and after migration to be affiliated to the same group in either the primary or the partner system is unclear. For example, Figure 10.16.2.2-1 seems to show that the late call entry is triggered by the server in the partner system (that would mean that the group is hosted there no matter steps 1 and 3 covering both primary/partner hosting options).

10.1.3 Unclear role of "MC Service FA Controlling Server" during Private call using functional alias towards a partner MC system

Clause 10.16.3.3 in 3GPP TS 23.280 depicts a situation where the FA resolution procedure is forwarded from a -so called- FA controlling server in the primary system to the service FA controlling server in the partner. However Stage 3 (i.e. Section 11.1.1.3.1.1 in 3GPP TS 24.379) defines that the initial INVITE will be submitted to the PSI of the Controlling server associated with the originating user's MCPTT ID identity (step 6) (therefore not with the called FA) and from there, according to step 8a) in 11.1.1.4.2 will initiate the FA resolution mechanism (9A.2.2.2.8). Therefore, the FA resolution mechanism would be triggered by the Controlling in the primary system serving the calling MCPTT-ID and forwarded directly to the one owning the FA in the partner system (making step 4 unneeded).

Same happens with the notification and selection of prime target in Step 7.

Step 4 & 7 in the Figure 10.16.3.3-1 and the role of the so-called FA resolution servers in migration scenarios (or in general in primary+partner systems) should be further clarified.

10.1.4 Behaviour upon “300 Multiple Choices” message in private call to a FA

During the definition of [CONN-MCPTT/ONN/PRIV/MIG/01] how both the controlling responsible for the caller, its participating and the MCPTT client handle the SIP 300 message is not explicitly described in 3GPP TS 24.379 (only for pre-established session behaviour is somewhere mentioned).

10.1.5 Ambiguity in the handling of the forwarding message for migrated users

Clause 4a in 11.1.1.3.2 in 3GPP TS 24.379 states that, if the MCPTT ID present in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body is marked as migrated to a partner system, then the terminating participating will generate a SIP MESSAGE request as described in clause 6.3.2.6 to trigger the call forwarding of a private call and shall include in the <anyExt> element of the <mcptt-Params> element of the <mcpttinfo> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body with the following clarification, a <forwarding-reason> element set to a value of "migrated" and <forwarding-target-orig-id> element set to the MCPTT ID in the partner system bound to the primary MCPTT ID at the migration authorization but the content of the RLS later needed by the controlling to process the forwarding message accordingly is not mentioned.

10.1.6 Ambiguity in the handling by the controlling server of new users/users to be removed from an ongoing adhoc MCPTT group emergency alert

Clauses 12.1A.2.6 and 12.1A.3.6 for adhoc MCPTT group emergency alert in 3GPPT TS 24.379 reuse the existing mechanisms (17.3.5.2.1 and 17.4.5.2.1 respectively) for updating the list of users during an adhoc MCPTT group call in the participating and controlling respectively. However, for the latter, the existing mechanisms entails according to step 4 c) inviting each of the MCPTT users determined above to the adhoc group session, as specified in clause 17.4.2.1.1. That is using an INVITE which does not apparently match the behaviour of the emergency alert in the terminating sides (neither in the participating nor in the client).

10.1.7 Clarification regarding the definition of the IWF for adhoc group call assuming MCPTT-aware-SIP only LMR side unlike any other group call or unclear mixture of client and participating roles

Step 1 a) in clause 10.1A.2.1.1 (and many other steps in the same clause) in 3GPP 29.379 unlike for example clause 10.1.3.1.1 assumes that the LMR side of the IWF uses SIP and even mcptt-info bodies.

Clause 10.1A.1.1 (client side) could be internally used but it is not explicitly referred in the participating clause but to specify the handling of 200 OK messages. Additionally, adhoc-grp-emg-alert-grp-ind is just one of the options considered.

10.1.8 Unclear reference (possibly a typo) to the participants determination procedure in adhoc group calls

Step 12 ii) in 3GPP TS 24.379 states that “the controlling will determine the users as specified in clause 17.4.5” that is actually used for the modification of participants and not for the determination (that would be 17.4.6).

10.1.9 Adhoc group emergency notification

Clause 6.2.0.1 in 3GPP TS 24.379 introduces the concept of SIP MESSAGE request for adhoc group emergency notification by using <adhoc-emergency-alert-ind> element but this is never again used and adhoc-alert-ind used instead.

Similarly, the reference in F.1.3 19 ba) in TS 24.379 stating “<adhoc-emergency-ind-rcvd> element set to: i) "true" and included in a SIP MESSAGE to indicate that the in-progress adhoc emergency cancellation request was received successfully;” seems to be deprecated/not matching.

10.1.10 Missing combined adhoc group call + emergency alert

Following Observation in 10.1.9, Table G.20-1 in 3GPP TS 24.379 states that “emergency alerts can be requested in several ways: MCPTT adhoc group emergency alert request with < adhoc-alert-ind> set to “true” or MCPTT emergency group call request with <adhoc-alert-ind> set to “true”. The latter would provide support for the combined group call and emergency alert in the pre-FRMCS#5 Plugtests / preRelease18 FRMCS 10.1 and 10.3 test cases functionality but such behaviour is never again mentioned.

10.1.11 Semantics and meaning of entity id in poc-settings

Section 7.4.1.2.2 in 3GPP TS 24.379 indicates the selected MCS user profile at an MC client defines the format for the entity in poc-settings. Whether the entity id needs to be MCS (Client) ID or MCPTT/MCData/MCVideo ID or any other... is not explicitly indicated and, since the XSD schema does not mandate a clarifying syntax different implementations from different vendors seem to understand it differently.

For example, according to 3GPP TS 29.283 clause 6.2.1.1 the general MC Service ID User-Identifier (in clause 7.3.8) contains the MC Service ID of the MC Service user for whom the data is required. So such entity id could be assimilated to User-Identifier in the UDB and therefore MC Service ID of the MC Service User.

However, r, in other parts of 3GPP TS 24.379 the entity id could be “client identifier”, since in section 7.2.4) there is the following reference “the <am-settings> element of the poc-settings+xml MIME body for each MCPTT client identified by the "id" attribute according to IETF RFC 4354 [55] as the current Answer-mode indication of that MPCTT client. That “that” would instead mean the id identifies the MCPTT Client (and not the user).

10.1.12 Wrong reference to RFC7253 for IDMS token handling

Section 6.2.3 step 2 b) i) in 3GPP TS 24.482 references to RFC7253 and it should reference to RFC7523.

10.2 Technical constraints

None identified in 5th FRMCS Plugtests.

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 Presentations

Observer programme is a presentation program during FRMCS Plugtests event which focused on the deployment plans and challenges of mission critical services for the railways.
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 presentations was conducted during half a day on Tuesday, 28th October 2025. The speakers presented to program outlined in Table 15.
Presentation slides in the observer program and the Questions & Answers are available on the Plugtests WIKI.

Presentations included:

Moderator – Guillaume Gach / UIC- Tuesday 28th Oct 2025		
Program	**Name/Organisation**	**Allocated Time**
Welcome and Agenda	Guillaume Gach / UIC	09:30
FRMCS V3 Specification Work frame	Dan Mandoc / UIC	09:40 - 10:00
Status on Finnish Digirail	Junttila Kari / Erillisverkot	10:00 - 10:20
Infrastructure Managers as FRMCS Service Providers	Sadaf Khan / Trafikverket	10:20 – 10:40
Coffee Break – 20 mins		
Status Update on MCX Certification	Harald Ludwig / TCCA	11:00 - 11:20
Discuss Deployment strategies and migration approaches towards FRMCS	Jesús Santiago / ADIF	11:20 – 11:50
Summary of rail outlook/trends in ANZ	Kevin Graham / TCCA	11:50 – 12:10
Status report Virve 2.0	Junttila Kari / Erillisverkot	12:10 - 12:30
Special Session on Band N100/101 - Qualcomm (30 mins) 12:30 – 13:00		
Lunch - 13:00 to 14:00		

Table 15. Observer Presentations

11.3 Observer Round Table Discussion

Observer round table discussions were organised on 29th October 2025 during FRMCS Plugtests event which focused on sharing of ideas, strategies, deployment challenges, conformance testing and performance of mission critical networks during the deployment.

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 Thursday, 30th October 2025. The following demos were presented:

FRMCS#5 Plugtests Observer Interop Demos

28 Oct 2025, 12:30-13:00 & 30 Oct 2025, 9:30-13:00

Demo#	Time Slot#	Room	Date	Time	Other vendors may watch	Alea	Alstom	Crosscall	Cybertel	Druid	Eviden	Frequentis	Funkwerk	Kontron	Funkwerk*	Leonardo	MCLabs	Nemergent	Qualcomm	Softil	Telematix	Teltronic	Valid8
08	T08	Test	28.Oct.25	12:30 – 13:00	Y									X					X				
05	T01	Test	30.Oct.25	09:30 – 10:20	Y									X					X		X		
04	T02	Obs	30.Oct.25	10:30 – 10:50	N		X		X	X												X	
01	T03	Obs	30.Oct.25	10:55 – 11:15	N	X		X	X			X						X				X	
02	T04	Obs	30.Oct.25	11:20 – 11:40	N			X									X					X	
03	T05	Obs	30.Oct.25	11:45 – 12:05	N			X												X		X	
06	T06	Obs	30.Oct.25	12:15 – 12:35	N	X		X								X				X		X	
07	T07	Obs	30.Oct.25	12:40 – 13:00	N			X			X						X				X	X	X

Table 16. Observer Demos

12 Interoperability Implementation Guide

The FRMCS and MCX Plugtests test case document (ETSI TS 103 564) specifies interoperability tests with the purpose of supporting those series of events. It therefore follows ETSI Interoperability best practices, including the identification of requirements specific methods, techniques and tools to be used, the naming conventions including test components and test purposes, the definition of test purposes, among others.

As part of the testing methodology, whenever an ambiguity or gap in the standards is identified a so-called observation is collected and conveyed to the relevant working group in the standardization organisation for clarification. However, even with a common understanding of the interfaces and standards to be evaluated during the interoperability tests, some practical or implementation questions arise that may have an impact into not only the interoperability testing carried out during the Plugtests themselves but also while deploying FRMCS systems in multivendor scenarios. The following list summarizes some of the findings during the 5th FRMCS Plugtests.

- **Handling of SIM cards**. Due to the large number of participants and 5GC providers, the number of SIM cards and the eventual need to swap them for different test sessions depending on the number of UEs available per FRMCS client vendor demand a careful handling and tracking by the participants. Although no issues or complains were finally reported to the ETSI team an unified or systematic approach for the abovementioned handling is deemed useful.
- **Need for frequency management**. The deployment of 5 different 5G radio equipment required a proper management of the spectrum to be used, requesting the proper permission to the spectrum regulator and coordinating in specific frequency bands.
- **Usage of specific test-related PLMN IDs**. Some commercial devices either ban or already have an OEM hard-coded configuration for test PLMN IDs (such as 001 01). This was announced in advance but, anyway, some 5GC providers decided to change the typical configuration to prevent any problems during the face to face event.
- **Provisioning information**. In the internal WIKI page for the 5th FRMCS Plugtests (https://wiki.plugtests.net/5th-FRMCS-Plugtests/index.php?title=Provisioning_Information) specific provisioning information is shared to help the interoperability and reduce the preparation needed for every test session, including adhoc calling criteria according to UIC FIS document, PLMN IDs to be used, N5 testing approach for AS providers, details for the domains/realms, Application Servers information, and conventions for SIP/IMS and MCX identities and functional aliases. However, the availability of bootstrapping mechanisms, the usage of Managed Objects –MOs- according to ETSI TS 124 383 or the adoption by the vendors of off-line (i.e. using MDM/OTA/TP or any other) automated provisioning method is not homogeneous in vendor implementations, making the final configuration mechanism mostly manual and therefore slow and error prone.
- **Role of the SIP/IMS cores and SIM cards**. Similarly to the previous, the usage of SIM based authentication and derivation of SIP identities and realms from the ISIM within the physical SIM card for SIP registration and IMS-AKA based authentication is still not available in many FRMCS clients/UE vendors. Similarly, the automated discovery of P-CSCF from the 5G network signalling was not widely used. Instead, manual configuration for every SIP/IMS core registrar server was needed.

- **MTU and fragmentation issues**. The testing setups typically involve connecting to components in different networks (5G, ethernet, VPN) even remotely through ETSI hive, with different MTU sizes. Since there is no agreed PMTU discovery mechanism in place and sometimes the FRMCS components do/can not properly control the Don't Fragment (DF bit) capabilities in IP datagrams there typically appear hard-to-troubleshoot connectivity issues. Although such issues were also announced and reminded to the participants it was still present during the event.

History

Document history		
V0.0.1	31/10/2025	First Draft
V0.0.2	17/11/2025	Stable Draft
V0.0.3	19/11/2025	Final Draft
V0.1.0	21/11/2025	Final Draft ready for publishing
V1.0.0	24/11/2025	Report published