ETSI Plugtests Report V1.1.0 (2018-10)

2nd ETSI MCPTT Plugtests
College Station, Texas, USA
25 – 29 June 2018

Keywords

Testing, Interoperability, Mission-Critical, LTE, MCPTT

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

Important notice

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Contents

Executive Summary

The capabilities of Mission Critical Push to Talk (MCPTT), Mission Critical Data (MCData) and Mission Critical Video (MCVideo) were tested during the week of the second MCPTT Plugtests on 25-29 June 2018 in College Station, Texas. More than 300 combinations of vendors and equipment, based on 3GPP Release-14, were tested.

The second ETSI MCPTT Plugtests attracted a total of 31 vendors (full list below), with 120 participants on site, plus support from remote labs. Observers from nine organizations based in France, the UK and the USA witnessed the execution of more than 2000 tests, based on a test plan with more than 100 test cases, with a 92 per cent success rate. The updated test specification with the newly added MCPTT Plugtests test scenarios will go through ETSI Technical Committee TCCE for approval and will become part of ETSI TS 103 564.

Building on the first MCPTT Plugtests in June 2017 in Sophia Antipolis, France, this second Plugtests event was conducted in College Station, Texas, to show the global approach of the technology. The Plugtests are the first of the series to evaluate public safety and mission critical Long Term Evolution (LTE) features and the interoperability of MCX products and services. For the first time in the world MCData and MCVideo have been tested. The goal is to validate the 3GPP standards, provide a platform for vendors to test their implementation and products, and ultimately achieve a single, interoperable, global standard.

The 2018 MCPTT Plugtests were hosted by the Texas A&M Internet2 Technology Evaluation Center (ITEC) at the Disaster City in College Station, Texas. The event was organized by ETSI, and supported by TCCA, the representative body for the global critical communications community, by the National Institute for Standards and Technology (NIST) Public Safety Communications Research (PSCR), the Public Safety Technology Alliance (PSTA) and the European Commission. FirstNet also took a great interest in the second MCPTT Plugtests.

The following equipment was tested:

MCPTT Application Servers (17 vendors):

- Airbus
- Alea
- Cisco
- Ericsson
- Genaker
- Frequentis (participating AS integrated in Control Room)
- Harris Corporation
- Huawei
- Hytera
- Kapsch CarrierCom
- Leonardo
- Motorola Solutions
- Nemergent
- Nokia
- StreamWIDE
- TASSTA
- TD Tech

MCVideo Application Servers (7 vendors):

- Alea
- Ericsson
- Genaker
- Harris Corporation
- Hytera
- Nemergent
- StreamWIDE

MCData Application Servers (10 vendors):

- Airbus
- Alea
- Ericsson
- Genaker
- Harris Corporation
- Hytera
- Kapsch CarrierCom
- Leonardo
- Motorola Solutions
- Nemergent

MCPTT Clients (20 vendors):

- Airbus
- Alea
- Armour Communications
- Etelm
- Funkwerk
- Genaker
- Harris Corporation
- Huawei
- Hytera
- Kapsch CarrierCom
- Leonardo
- Mission Critical Open Platform (MCOP)
- Nemergent
- Nokia
- Prescom
- Softil
- Sonim
- TASSTA
- TD Tech
- Valid8

MCVideo Clients (8 vendors):

- Alea
- Funkwerk
- Genaker
- Harris Corporation
- Hytera
- Nemergent
- Nokia
- Softil

MCData Clients (8 vendors):

- Airbus
- Alea
- Etelm
- Genaker
- Harris Corporation

- Hytera
- Leonardo
- Softil

Evolved Multimedia Broadcast Multicast Services (eMBMS) Components (5 vendors):

- Athonet
- Expway
- ENENSYS Technologies
- Huawei
- one2many

LTE network components (3 vendors):

- Athonet
- Ericsson
- Expway

User Equipment (6 vendors):

- Airbus
- Bittium
- Funkwerk
- Huawei
- Sonim
- TD Tech

IP Multimedia Subsystem (IMS) (1 vendor):

- Athonet

Audio Quality Tester (1 vendor):

- Spirent

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

The next MCX Plugtests event is planned for Q4 2018.

1 Introduction

Push-to-Talk (PTT) is a standard feature of narrowband Professional Mobile Radio (PMR) technologies developed specifically for mission-critical communications. PTT enables near instantaneous group communications – a critical requirement in an emergency situation. It is used in many systems like TETRA or P25 and mission critical networks today worldwide.

Mission Critical PTT (MCPTT) is a standardized voice service for LTE systems which ensure that LTE and 5G systems support mission-critical communications.

Although the PMR market shows no signs of slowing, mission-critical broadband will offer complementary capabilities, and its market is expected to grow at a compound annual growth rate of 20 per cent, from $1.1 billion in 2015 to $2.6 billion in 2020, according to IHS Market. The first nationwide rollouts in the United States, South Korea, the UK, the Middle East and Asian countries are expected to trigger significant large-scale investments in mission-critical LTE.

Mission Critical Push To Talk (MCPTT) was the first of a number of Mission Critical features which was finalized by the 3GPP working group SA6 in Release-13. Mission Critical Video and Mission Critical Data were finalized in Release-14 by 3GPP working group SA6.

Preparations for the second Plugtests event started in January 2018 with the registrations of vendors and observers. During bi-weekly conference calls from January to June 2018 the setup of the tests, the test specification and organizational issues were agreed between the participants. Before the actual face-to-face tests end of June 2018, the vendors have been done 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 2nd MCPTT 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 2nd MCPTT Plugtests event wiki: https://wiki.plugtests.net/wiki/2nd-MCPTT-Plugtests (login required). Clause 4 describes the management of the Plugtests event.

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

- MCPTT Application Servers (AS)
- MCData Application Servers (AS)
- MCVideo Application Servers (AS)
- MCPTT Clients
- MCData Clients
- MCVideo Clients
- User Equipment (UE)
- LTE network components: Evolved Packet Core (EPC), Evolved Node B (eNB) and Multimedia Broadcast Multicast Service (eMBMS)
- IP Multimedia Subsystem (IMS)
- Broadcast Multicast Service Center (BMSC)
- Audio Quality Tester

The remote pre-test and on-site test infrastructure is described in clause 6; the test procedures are described in clause 7.

In April and May 2018 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 MCPTT. During May-June2018 the vendors conducted pre-tests with each other.

ETSI has developed a test specification with 100 test cases. See clause 8. The test specification will be published as an update of ETSI document ETSI TS 103 564.

About 2000 tests were conducted by the vendors. 92% of the tests were successful, the remaining 8% failed for various reasons. The detailed results of the tests are available for the involved vendors in these tests, but are not disclosed to the other vendors or to the public. All participants had to sign a Non-Disclosure Agreement before joining the Plugtests event. The statistics of the test results are listed in clause 9.

The failed tests give the vendors valuable information to improve their implementations. They also help to discover ambiguities in the standards and to clarify and improve the specifications. The observations from the Plugtests event are fed back to the 3GPP working groups. The observations are listed in clause 10

ETSI plan to conduct more MCX Plugtests in the future. The next MCX Plugtests sessions are planned for Q4 2018. Vendors who have not participated in the first or second MCPTT Plugtests events are welcome and encouraged to join the next MCX Plugtests event. The interest of TCCA and ETSI is to have one global standard for Mission Critical services, which can be ensured by interoperability testing at the Plugtests.

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 versions for the second Plugtests. Please see also the test specification document for the references.

[1] ETSI TS 103 564: TCCE; Testing; Plugtest™ scenarios for Mission Critical Push To Talk (MCPTT)

[2] 3GPP TS 22.179: Mission Critical Push to Talk (MCPTT) over LTE; Stage 1, Release 14, Version 14.3.0, December 2016.

[3] 3GPP TS 23.280: Common functional architecture to support mission critical services; Stage 2, Release 14, Version 14.4.0, January 2018

[4] 3GPP TS 23.379: Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2, Release 14, Version 14.4.0, Jan 2018.

[5] 3GPP TS 23.468: Group Communication System Enablers for LTE (GCSE_LTE); Stage 2, Release 14, Version 14.0.0, March 2017.

[6] 3GPP TS 24.229: IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), Release 14, Version 14.6.0, Dec 2017.

[7] 3GPP TS 24.281: Mission Critical Video (MCVideo) signalling control; Protocol specification, Release 14, Version 14.2.0, December 2017.

[8] 3GPP TS 24.282: Mission Critical Data (MCData) signalling control; Protocol specification, Release 14, Version 14.2.0, December 2017.

[9] 3GPP TS 24.379: Mission Critical Push To Talk (MCPTT) call control; Protocol specification, Release 14, Version 14.4.0, December 2017.

[10] 3GPP TS 24.380: Mission Critical Push To Talk (MCPTT) media plane control; Protocol specification, Release 14, Version 14.5.0, December 2017.

[11] 3GPP TS 24.481: Mission Critical Services (MCS) group management; Protocol specification, Release 14, Version 14.3.0, December 2017.

[12] 3GPP TS 24.482: Mission Critical Services (MCS) identity management; Protocol specification, Release 14, Version 14.2.0, December 2017.

[13] 3GPP TS 24.483: Mission Critical Services (MCS) Management Object (MO), Release 14, Version 14.3.0, December 2017.

[14] 3GPP TS 24.484: Mission Critical Services (MCS) configuration management; Protocol specification, Release 14, Version 14.4.0, December 2017.

[15] 3GPP TS 24.581: Mission Critical Video (MCVideo) media plane control; Protocol specification, Release 14, Version 14.3.0, March 2018 -Check NOTE-.

[16] 3GPP TS 24.581: Mission Critical Video (MCVideo) media plane control; Protocol specification, Release 14, Version 14.3.0, March 2018 -Check NOTE-.

[17] 3GPP TS 24.582: Mission Critical Data (MCData) media plane control; Protocol specification, Release 14, Version 14.2.0, December 2017.

[18] 3GPP TS 26.179: Mission Critical Push To Talk (MCPTT); Codecs and media handling, Release 14, Version 14.0.0, March 2017.

[19] 3GPP TS 26.346: Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs, Release 14, Version 14.5.0, January 2018.

[20] 3GPP TS 29.212: Policy and Charging Control (PCC); Reference points; Release 14, Version 14.6.0, Dec 2017.

[21] 3GPP TS 29.214: Policy and Charging Control over Rx reference point; Stage 3, Release 14, Version 14.6.0, Dec 2017.

[22] 3GPP TS 29.283: Diameter Data Management Applications, Release 14, Version 14.3., September 2017.

[23] 3GPP TS 29.468: Group Communication System Enablers for LTE(GCSE_LTE); MB2 reference point; Stage 3, Release 14, Version 14.3.0, December 2017.

[24] 3GPP TS 33.180: Security of the mission critical service, Release 14, Version 14.2.0, January 2018.

[25] IETF RFC 3515: The Session Initiation Protocol (SIP) Refer Method, April 2003.

[26] IETF RFC 3856: A Presence Event Package for the Session Initiation Protocol (SIP), August 2004.

[27] IETF RFC 3903: Session Initiation Protocol (SIP) Extension or Event State Publication, October 2004.

[28] IETF RFC 4488: Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription, May 2006.

[29] IETF RFC 4825: The Extensible Markup Language (XML) Configuration Access Protocol (XCAP), May 2007.

[30] IETF RFC 5366: Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP), October 2008.

[31] IETF RFC 5373: Requesting Answering Modes for the Session Initiation Protocol (SIP), November 2008.

[32] IETF RFC 5875: An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Diff Event Package, May 2010.

[33] IETF RFC 6135: An Alternative Connection Model for the Message Session Relay Protocol (MSRP), February 2011.

[34] IETF RFC 6665: SIP-Specific Event Notification, July 2012.

[35] IETF RFC 7647: Clarifications for the use of REFER with RFC6665, September 2015.

[36] OMA. OMA-TS-XDM_Core-V2_1-20120403-A: XML Document Management (XDM) Specification, V2.1, April 2012

[37] OMA. OMA-TS-XDM_Group-V1_1_1-20170124-A: Group XDM Specification, V1.1.1, Jan 2017

3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [27] 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 [27].

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
EPC	Evolved Packet Core
EPS	Evolved Packet System
ETSI	European Telecommunications Standard Institute
EUT	Equipment Under Test
FD	File Distribution
FE	Functional Element
GCSE	Group Communication Service Enabler
GMK	Group Master Key
GMS	Group Management Server
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
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
OTT	Over the Top
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
TAMU	Texas A&M University
TCCA	The Critical Communications Association
TD	Test Description
TR	Technical Recommendation
TRT	Test Reporting Tool
TS	Technical Specification
UE	User Equipment

4 Technical and Project Management

4.1 Scope

The main goal of the second MCPTT Plugtests was testing the interoperability of the MCPTT, MCData and MCVideo ecosystem signalling and media plane at different levels.

The basic scenario tested comprised MCX application server(s) -both controlling and participating- and MCX clients deployed over a generic SIP Core/IMS, LTE access network with and without MCPTT required PCC capabilities with native multicast support (i.e. Release-13 eMBMS) and UEs. The following figure (Fig 1) illustrates the basic test infrastructure.

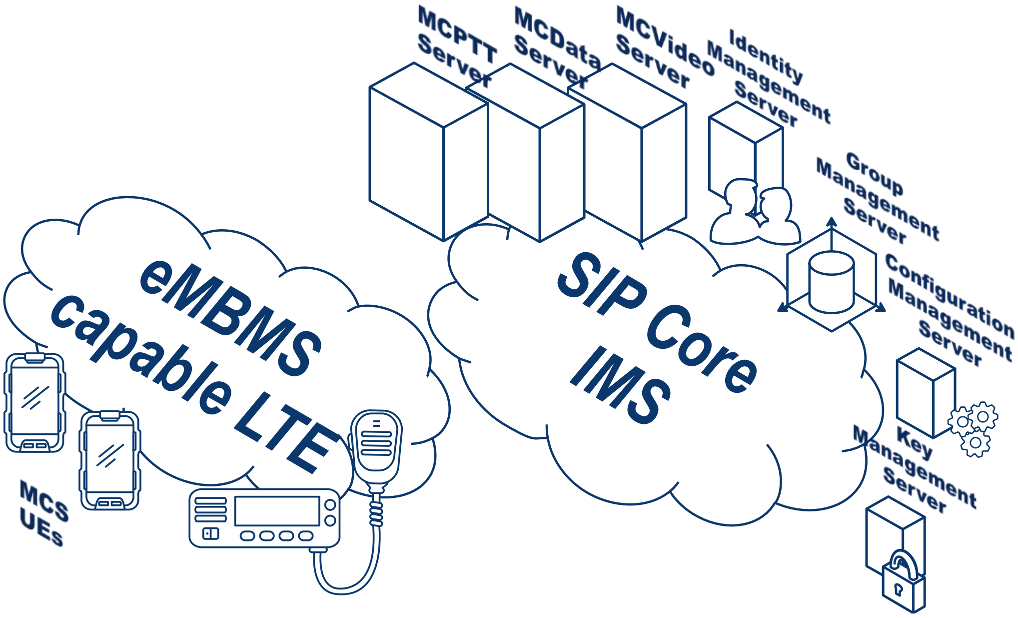

Figure 1. Typical MCPTT/MCData/MCVideo scenario to be considered in the Plugtests

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

- **Connectivity (CONN)**: Tests covered basic connectivity between functional elements at different levels including Access Network (LTE), IP Network, SIP/IMS and MCPTT/MCData/MCVideo Application level. At LTE level, unicast and more particularly eMBMS multicast connectivity was evaluated. IP layers targeted pure OTT connectivity regardless the underlying access network. SIP connectivity tests checked proper deployment of MCPTT AS over the selected SIP Core/IMS so that all SIP messages were successfully delivered from MCPTT Clients to Participating/Controlling MCPTT Servers and vice versa. In this 2nd Plugtests some AS vendors provide their own SIP/IMS cores so that Clients registered into different cores depending of the specific test case. Application level refers to e2e signalling, media, floor controlling (and other involved) protocols in use. Although all CONN tests could be tentatively evaluated over all the different configurations (Over-The-Top – or OTT – Mission Critical LTE for unicast – or UNI-MC-LTE – and Mission Critical LTE with multicast eMBMS-capabilities – so called MULTI-MC-LTE - see Clause 8) most tests used the OTT one for its flexibility and the possibility of scheduling parallel test easily. Additionally, low level configuration-specific details (i.e. MCPTT. MC QCI and eMBMS bearer management) were considered in the PCC and eMBMS specific objectives. An additional set of optional eMBMS tests were also evaluated. Note that 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.

- **Policing (PCC)**: Comprised specific checking proper LTE dynamic bearer signalling and allocation by eUTRAN/EPC.
- **eMBMS (EMBMS)**: Comprised checking of eMBMS specific signalling.
- **Registration and authorization (REGAUTH)**: Comprised MCPTT Client registration.
- **Affiliation (AFFIL)**: Comprised MCPTT Client explicit and implicit affiliation
- **Location (LOC)**: In the test specification document several location configuration, retrieval and submission procedures were considered..
- **OAM procedures (CSC):** Comprised OAM related IdMS, CMS, GMS and KMS interfacing procedures. Mostly MCPTT mechanisms were evaluated since MCData/MCVideo implementations were not as mature as MCPTT implementations and are also mainly equivalent to MCPTT implementations.
- **Security (SEC):** Comprised security related procedures (mainly cyphering and some preliminary key retrieval considered in KMS-related test cases in CSC test cases).

Finally, note that, since Release-14 was evaluated during this 2nd Plugtests, a particular effort was devoted to check whether the updated Release-13 mechanisms were consistent considering new configuration files and data formats.

4.2 Timeline

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

Figure 2. Plugtests event timeline

Registration to the MCPTT Plugtests event was open from 15th February 2018 to 15th March 2018 to any organisation willing to participate in testing the MCX Services Ecosystem. Additional remote participation (i.e. back office support) was possible and supported with electronic tools, see clause 4.3. A total of 120 people were finally involved onsite in the face-to-face part of the Plugtests event plus remote labs.

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 face-to-face 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. The Test Plan was scoped around 3GPP Test Specification Release-14 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 Remote integration & pre-testing

Starting in April 2018, participants connected their implementations remotely to the Plugtests event infrastructure, known as HIVE: Hub for Interoperability and Validation at ETSI.

During this phase, up to 31 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 face-to-face Plugtests event time and smoother Interoperability Test Sessions.

A VPN connection to HIVE was highly recommended for participants providing MCX servers, MCX Clients and IMS 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.

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 25th of June to the 29th of June 2018, participants sent representatives to the host Lab in College Station, Texas to collaboratively run the Interoperability Test Sessions. The Plugtests were kindly hosted by the Texas A&M University at their extension facilities in the Disaster City.

This one-week on-site face-to-face event was scheduled as follows:

MCPTT#2 PLU Agenda (25 - 29 June 2018)						
Time	Sunday 24	Monday 25	Tuesday 26	Wednesday 27	Thursday 28	Friday 29
07:45		Room Opening	Room Opening	Room Opening	Room Opening	Room Opening
08:00 10:00		SET-UP / TEST SESSION #1	TEST SESSION #5	TEST SESSION #9	TEST SESSION #13	TEST SESSION #17
10:00 10:30		COFFEE BREAK	COFFEE BREAK	COFFEE BREAK	COFFEE BREAK	COFFEE BREAK
10:30 12:30		TEST SESSION #2	TEST SESSION #6	TEST SESSION #10	TEST SESSION #14	TEST SESSION #18
12:30 13:30		LUNCH BREAK	LUNCH BREAK	LUNCH BREAK	LUNCH BREAK	LUNCH BREAK
13:30 15:30	SET-UP FOR PARTICIPANTS 14:00 - 16:30	TEST SESSION #3	TEST SESSION #7	TEST SESSION #11	TEST SESSION #15	FINAL WRAP-UP
15:30 16:00		COFFEE BREAK	COFFEE BREAK	COFFEE BREAK	COFFEE BREAK	TEAR-DOWN STARTS AT 15:00
16:00 18:00		TEST SESSION #4	TEST SESSION #8	TEST SESSION #12	TEST SESSION #16	
18:00 18:30		WRAP-UP	WRAP-UP	WRAP-UP	WRAP-UP	
			Social event starts 19:15		Social event	

Figure 3. High-level schedule for Plugtests event on-site

Sunday and first half of Monday was dedicated to local installation and pre-testing continuation, this time also including local implementations. A number of EUTs were installed and connected locally to the HIVE infrastructure, as well as some test and support functions.

The following 4.5 days were dedicated to on-site interoperability test sessions involving all the participating EUTs organised in several parallel tracks, see details in Clause 4.3.2.

The scheduling of individual test combinations was done manually with the inputs and requests from the participants. 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 MCPTT 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.
- **Base and Test Specs -** High Level Test Scope including the test specification and reference to 3GPP and IETF specifications.
- **Registered Equipment** - Participating EUTs overview.
- **Supported Functionality -** Functionality supported by EUTs.
- **Testing Information -** Pre-configured parameters for EUTs.
- **Conference Calls** - Calendar, logistics, agendas and minutes of the bi-weekly conference calls run during the remote integration and pre-testing phase.
- **Test Reporting Tool** - Documentation of the Test Reporting Tool.
- **Plugtests Observations** - Issues found during Plugtests event.
- **Network Infrastructure** - HIVE connection request tool, and remote connections status overview.
- **Pre-Testing Schedule**- Pre-testing schedule, remote integration and pre-testing procedures.
- **Main Event Schedule** - Test session schedule for the main face-to-face event.

In addition, the embedded WIKI Chat and 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 on-site 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 sessions 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.

2017-06-20 16:00	120	Test Slot 4	Main_CONFIG 1	Athonet - IMS / SIP Core Alea - MCPTT AS Armour - MCPTT Client
2017-06-20 16:00	120	Test Slot 3	Main_CONFIG 2_eMBMS_OTT	Huawei - BM-SC Hytera - MCPTT AS
2017-06-20 14:00	120	Test Slot 5	Main_CONFIG 1	Athonet - IMS / SIP Core Tassta - MCPTT AS Spirent - MCPTT Client
2017-06-20 14:15	120	Test Slot 6	Main_CONFIG 1	Athonet - IMS / SIP Core Airbus - MCPTT AS Armour - MCPTT Client
2017-06-20 16:30	120	Test Slot 6	Main_CONFIG 1	Athonet - IMS / SIP Core Harris - MCPTT AS Airbus - MCPTT Client
2017-06-20 16:15	120	Test Slot 5	Main_CONFIG 6	Athonet - ePC + eNB Nemergent - MCPTT AS Nemergent - MCPTT Client Armour - MCPTT Client
2017-06-20 14:15	120	Test Slot 7	Main_CONFIG 1	Athonet - IMS / SIP Core Airbus - MCPTT AS Hytera - MCPTT Client
2017-06-21 11:00	120	Test Slot 6	Main_CONFIG 1	Athonet - IMS / SIP Core Airbus - MCPTT AS Genaker - MCPTT Client
2017-06-21 11:00	120	Test Slot 3	Main_CONFIG 1	Athonet - IMS / SIP Core Harris - MCPTT AS Etelm - MCPTT Client

Figure 4. Test Reporting Tool – example screen shot

5 Equipment Under Test

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

5.1 MCPTT Application Servers

Organisation	Comment
Airbus	–
Alea	Supports split operation as Participating AS and Controlling AS
Cisco	–
Ericsson	–
Genaker	–
Frequentis	Participating AS only; included in the Frequentis Control Room
Harris Corporation	–
Huawei	–
Hytera	Supports split operation as Participating AS and Controlling AS
Kapsch CarrierCom	–
Leonardo	Supports split operation as Participating AS and Controlling AS
Motorola Solutions	–
Nemergent	Supports split operation as Participating AS and Controlling AS
Nokia	–
StreamWide	–
TASSTA	–
TD Tech	–

Table 1. MCPTT Application Servers Under Test

5.2 MCVideo Application Servers

Organisation	Comment
Alea	Supports split operation as Participating AS and Controlling AS
Ericsson	–
Genaker	–
Harris Corporation	–
Hytera	Supports split operation as Participating AS and Controlling AS
Nemergent	Supports split operation as Participating AS and Controlling AS
StreamWide	–

Table 2. MCVideo Application Servers Under Test

5.3 MCData Application Servers

Organisation	Comment
Airbus	
Alea	Supports split operation as Participating AS and Controlling AS
Ericsson	–
Genaker	–
Harris Corporation	–
Hytera	Supports split operation as Participating AS and Controlling AS
Kapsch CarrierCom	
Leonardo	Supports split operation as Participating AS and Controlling AS
Motorola Solutions	
Nemergent	Supports split operation as Participating AS and Controlling AS

Table 3. MCData Application Servers Under Test

5.4 MCPTT Clients

Organisation	Comment
Airbus	–
Alea	–
Armour Communications	–
Etelm	included in the Etelm TETRA Base Station
Funkwerk	MCPTT Client on dedicated Cabradio-platform
Genaker	–
Harris Corporation	–
Huawei	–
Hytera	–
Kapsch CarrierCom	–
Leonardo	–
MCOP	(Mission Critical Open Platform)
Nemergent	–
Nokia	–
Prescom	–
Softil	–
Sonim	–
TASSTA	–
TD Tech	–
Valid8	–

Table 4. MCPTT Clients Under Test

5.5 MCVideo Clients

Organisation	Comment
Alea	–
Funkwerk	–
Genaker	–
Harris Corporation	–
Hytera	–
Nemergent	–
Nokia	–
Softil	–

Table 5. MCVideo Clients Under Test

5.6 MCData Clients

Organisation	Comment
Airbus	–
Alea	–
Etelm	–
Genaker	–
Harris Corporation	–
Hytera	–
Leonardo	–

Organisation	Comment
Softil	–

Table 6. MCData Clients Under Test

5.7 User Equipment (UEs)

Organisation	Comment
Airbus	–
Bittium	–
Funkwerk	Cab Radio
Huawei	–
Sonim	–
TD Techi	–

Table 7. User Equipment Under Test

5.8 IP Multimedia Subsystem (IMS)

Organisation	Comment
Athonet	–

Table 8. IP Multimedia Subsystem (IMS) Under Test

5.9 LTE Network Components

The organisations listed below provided the LTE Network Components for the Plugtest, i.e. Evolved Packet Core (EPC) and Evolved Node B (eNB).

Organisation	Comment
Athonet	–
Ericsson	–
Expway	–

Table 9. LTE Network Components Under Test

5.10 Evolved Multimedia Broadcast Multicast Services (eMBMS) Components

Organisation	Comment
Athonet	–
Expway	–
ENENSYS Technologies	–
Huawei	–
one2many	–

Table 10. Evolved Multimedia Broadcast Multicast Services (eMBMS) Components Under Test

5.11 Audio Quality Tester

Organisation	Comment
Spirent	–

Table 11. Audio Quality Tester

6 Test Infrastructure

6.1 Remote and Local Test Infrastructure

The remote integration and pre-testing phase was enabled by the setup as shown in Figure 5:

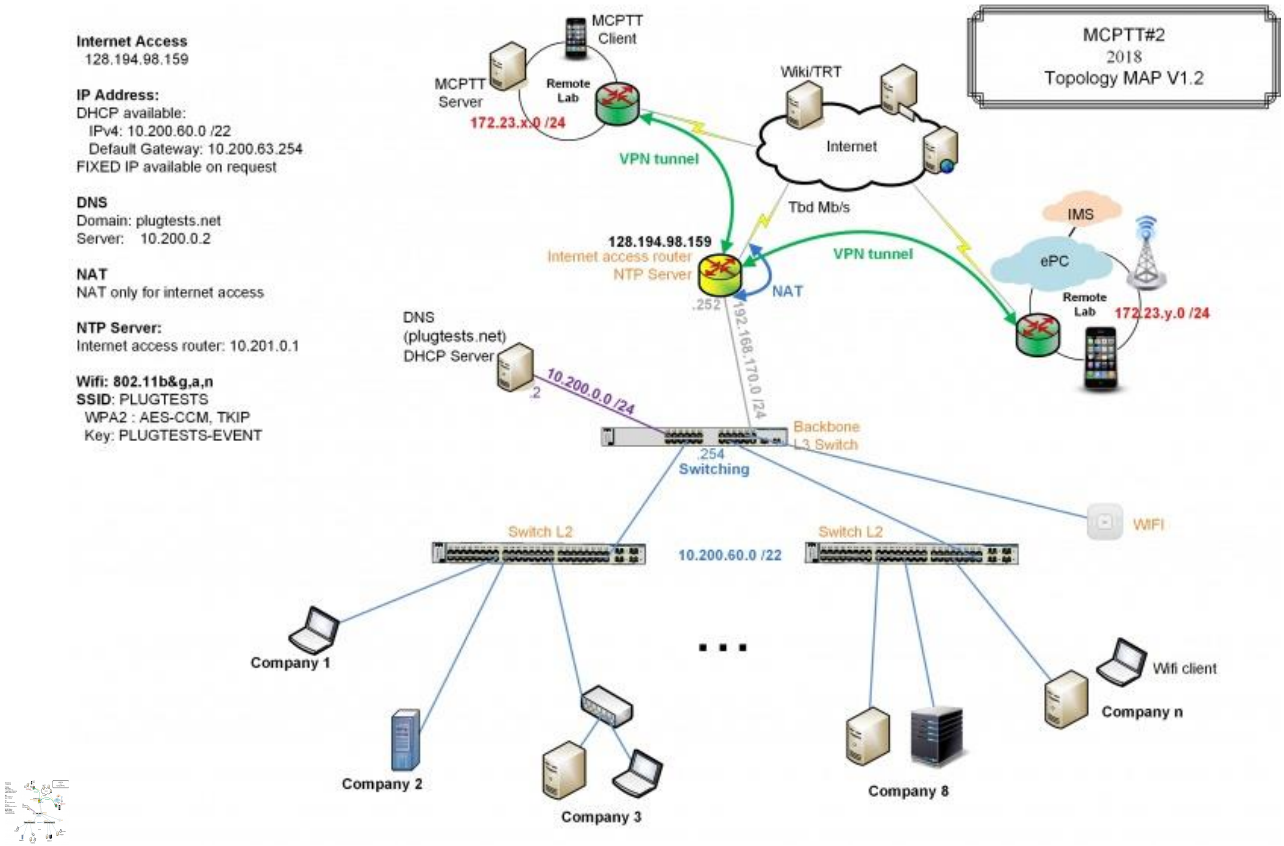

Figure 5. Remote Test Infrastructure

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 31 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_CONFIG 1	MCPTT Client + MCPTT AS (Participating + Controlling) + IMS / SIP Core
PreTest_CONFIG 2_MBMS	MCPTT Client + MCPTT AS (Participating + Controlling) + IMS / SIP Core + BM-SC
PreTest_CONFIG 3	MCPTT Client + MCPTT AS (Participating + Controlling) + IMS / SIP Core + LTE
PreTest_CONFIG 4_MBMS_OTT	MCPTT AS (Participating + Controlling) + BMSC

Table 12. Pre-testing Configuration

7.2 Interoperability Testing Procedure

During the on-site face-to-face part of the Plugtests event, a daily Test Session Schedule was produced and shared via the WIKI. 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.

Main Event Schedule

Test Combinations [edit]

Main Event Schedule : Main Event Test Combinations

Monday Morning							
Session#	TRT#	MCPTT Client	MCPTT UE	MCPTT AS	IMS / SIP Core	LTE	BMSC - MBMS
1 & 2	3298	Airbus		Leonardo	Leonardo		
1 & 2	3299	Softil		Airbus	Athonet		
1 & 2	3315	TDTech		Tassta	Athonet		
1 & 2	3301	Leonardo		Cisco	Athonet		
1 & 2	3302 / 3308	Prescom / Sonim		Kapsch	Kapsch		
1 & 2	3303	Nemergent		Nokia	Nokia		
1 & 2	3304	Nokia		Nemergent	Athonet		
1 & 2	3309 / 3305	MCOP / Harris		TDTech	TDTech		
1 & 2	3306	Armour		Motorola	Athonet		
1 & 2	3307	ETELM		Streamwide	Athonet		
1 & 2	3310	Hytera		Harris	Athonet		
1 & 2	3311	Kapsch		Alea	Alea		
1 & 2	3312	Alea		Alea			Enensys
1 & 2	3300	TDTech		Nemergent	Athonet		
1 & 2	3314	Prescom		Motorola	Athonet		
1 & 2	3313	Armour		Hytera	Hytera		
1 & 2	3316	Valid8		Streamwide	Athonet		

Figure 6. Daily Schedule & Test Sessions – example excerpt

Config Name	Main Test Configuration
Main_CONFIG 1	MCPTT Client + MCPTT AS (Participating+Controlling) + IMS / SIP Core
Main_CONFIG 2_eMBMS	MCPTT Client + MCPTT AS (Participating+Controlling) + IMS / SIP Core + BMSC + LTE
Main_CONFIG 3	MCPTT Client + MCPTT AS Participating + MCPTT AS Controlling + IMS / SIP Core
Main_CONFIG 4	LTE + MCPTT Client + MCPTT AS (Participating+Controlling) + IMS / SIP Core + UE
Main_CONFIG 5	MCPTT Client + MCPTT AS Participating + MCPTT AS Controlling + IMS / SIP Core + MCPTT Client
Main_CONFIG 6	MCPTT Client +MCPTT AS (Participating+Controlling) + IMS / SIP Core + MCPTT Client
Main_CONFIG 7 eMBMS	LTE + MCPTT AS (Participating+Controlling) + IMS / SIP Core + BMSC + MCPTT Client + UE
Main_CONFIG 8 MBMS OTT	BMSC + MCPTT AS (Participating+Controlling)
Main_CONFIG 9 Audio Testing	Audio Quality Tester + MCPTT Client
Main_CONFIG 10 Audio Testing	Audio Quality Tester + MCPTT Client + UE
Main_CONFIG 11	MCPTT Client + UE +MCPTT AS (Participating+Controlling) + IMS / SIP Core +

Config Name	Main Test Configuration
	MCPTT Client + UE + BMSC
Main_CONFIG 12	MCPTT Client + UE +MCPTT AS Participating+ MCPTT AS Controlling + IMS / SIP Core + UE
Main_CONFIG 13	MCPTT Client + MCPTT Client + IMS / SIP Core + MCPTT AS (Participating+Controlling)

Table 13. 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.

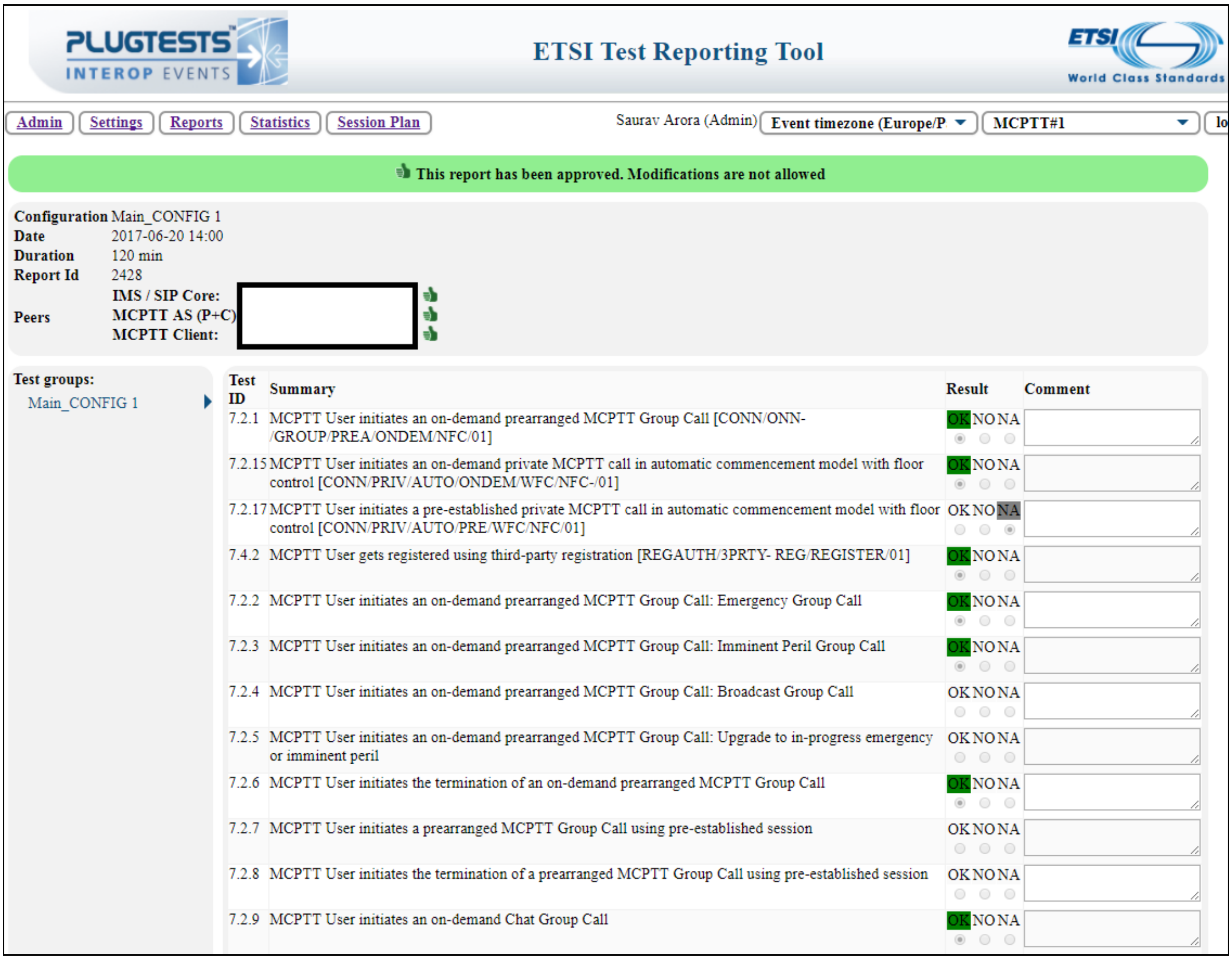

Figure 7. Test Session Report

2. For each Test in the Test Plan:

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

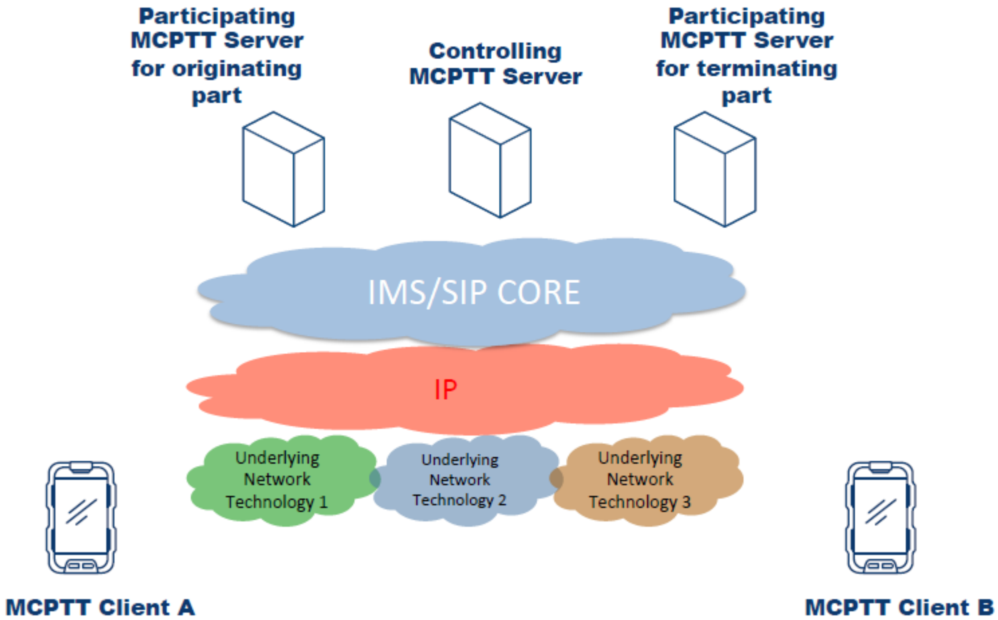

Figure 8. System Under Test (SUT) Configuration – MCPTT example

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 9. 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 2nd MCPTT Plugtests Test Plan was developed following ETSI guidelines for interoperability. It is based on the test plan from the 1st MCPTT Plugtests, amended by MCData, MCVideo and additional call types and procedures. Furthermore, the test cases from the 1st Plugtests, which were based on 3GPP Release-13, were upgraded to 3GPP Release-14.

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 first Plugtests and new companies, vendors selected the subset of test cases to evaluate in a per-testing slot basis.

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

8.2 Test configurations

The overall MCX ecosystem comprises both controlling and participating MCPTT/MCData/MCVideo application server(s), MCPTT Clients deployed over a generic SIP Core/IMS, LTE access network with and without MCPTT required PCC capabilities and native multicast support (i.e. Release-13 eMBMS). Furthermore, a series of support servers were integrated in the so-called Common Services Core provide configuration, identity, group and key management capabilities. Only 3GPP Release-14 compliant On-Network operations were considered.

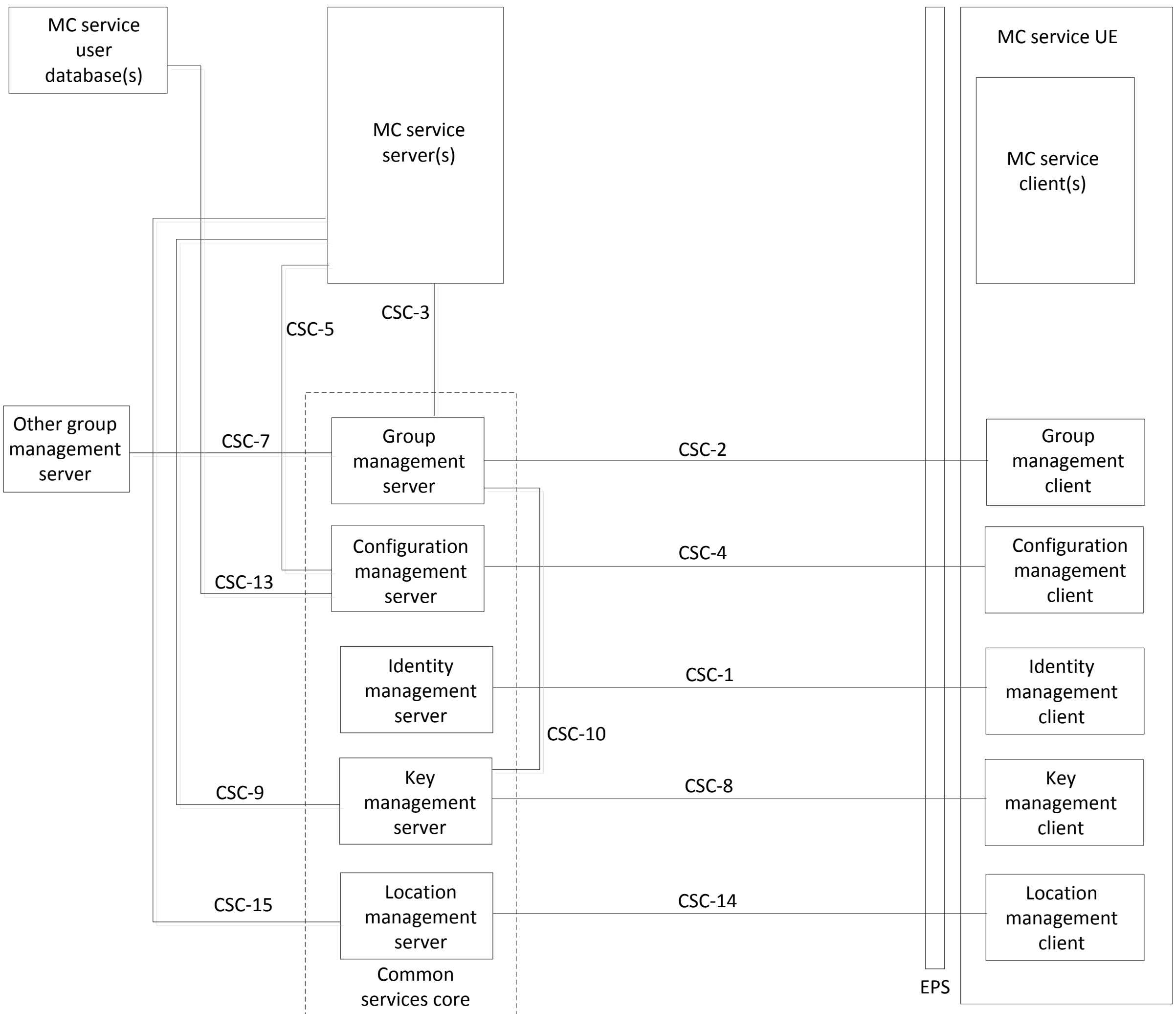

Figure 10. Functional model for application plane Figure 7.3.1-1 in 3GPP TS 23.280 [3].

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 Rx and MB2-C/MB2-U) involving other supporting technologies like LTE EPS. 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), unicast Mission Critical LTE and multicast Mission Critical LTE (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 LTE, 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 or multicast mechanisms in LTE). 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 LTE infrastructure and allowed both signalling and media plane parallel testing easily.

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

In this configuration the LTE network (both EPC and eUTRAN) 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 EPC/eUTRAN, and the availability of a PCRF with MCPTT compliant Rx/MCPTT-5 interface. Specific Rx/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.

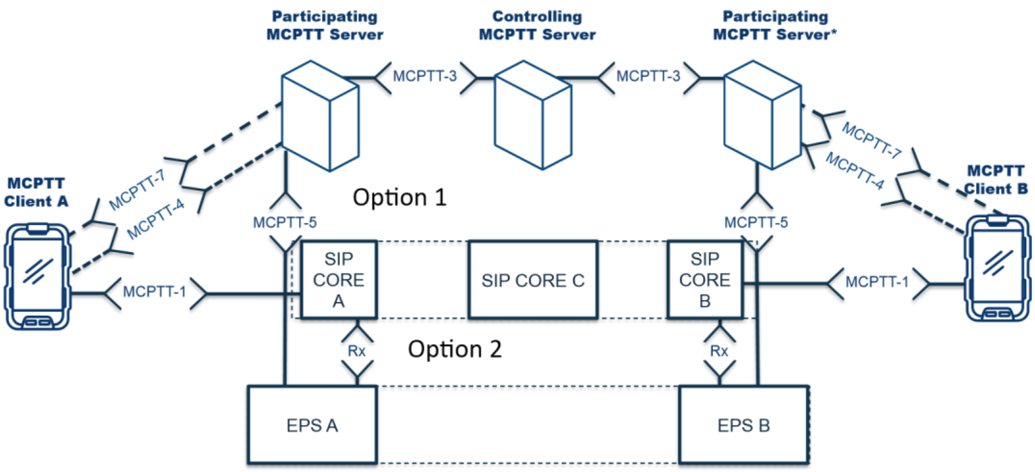

Figure 11. CFG_ONN_UNI-MC-LTE-1 configuration

8.2.3 Multicast Mission Critical LTE for On-Network calls (CFG_ONN_MULTI-MC-LTE-1)

In this configuration LTE provided multicast capability including Rel. 13 (and beyond) LTE-A Pro eMBMS and needed interfaces both in the core side (MB2-C and MB2-U with the BM-SC) and in the eUTRAN/UE side. It was used to test eMBMS bearer setup and update related test cases.

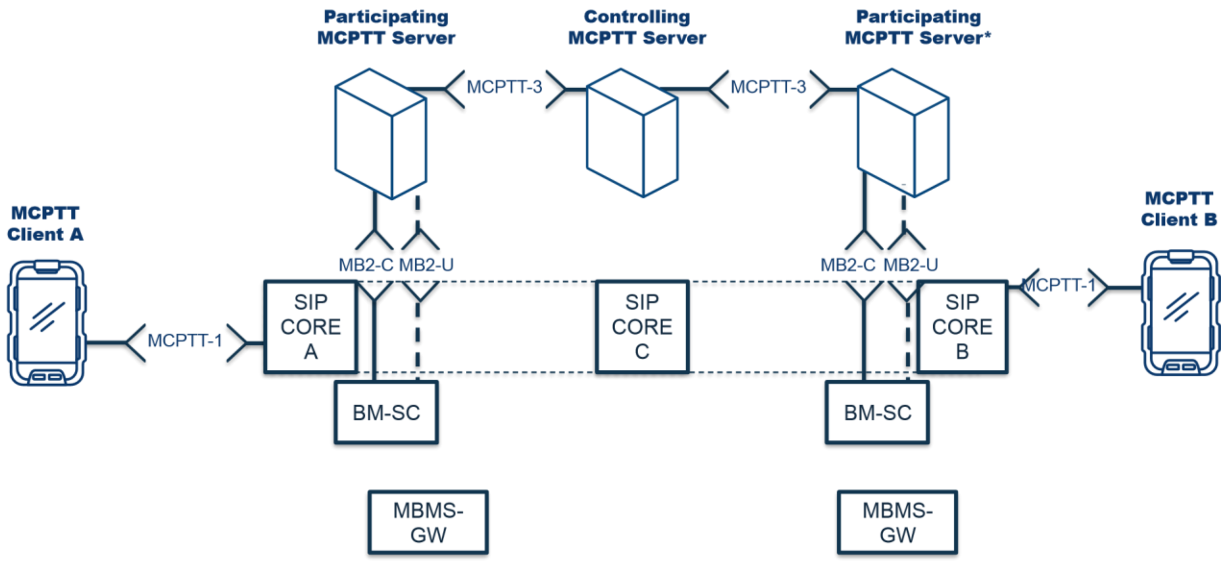

Figure 12. CFG_ONN_MULTI-MC-LTE-1 configuration

Due to specific low level technical constraints (i.e. the availability of joint/split participating and controlling AS, usage of MCPTT-5 interface instead of Rx for the PCC or eMBMS support in the UE) the original configurations led to the ones described in Figure 12 according to the following mapping.

Note that eMBMS_OTT refers to testing the eMBMS signalling in the MB2-C/MB2-U reference points and all the UE <-> MCPTT AS eMBMS triggering related signalling but with no eMBMS capable eUTRAN. Main_CONFIG 4 comprises MC QCI capable enodeB and UEs (and PCRF) and Main_CONFIG 7 the usage of alternative enodeB interfaces.

Configuration	Resulting configuration mode in the Plugtests (TRT)
ONN-OTT	Main_CONFIG 1
	Main_CONFIG 8_eMBMS_OTT
	Main_CONFIG 3
	Main_CONFIG 5
	Main_CONFIG 6
	Main_CONFIG 11
	Main_CONFIG 12
	Main_CONFIG 13
UNI-MC-LTE	Main_CONFIG 4
	Main_CONFIG 7
MULTI-MC-LTE	Main_CONFIG 2_eMBMS

Table 13. Mapping of scenario architecture configurations and Plugtests event practical configurations

8.2.4 Group of test cases

As described in the Subclause 4.1 of this document, different test objectives were considered.

In order to avoid bottlenecks, Connectivity (CONN), Floor Controlling (FC), Registration and authorization (REGAUTH) and Affiliation (AFFIL) objectives were tested on the ONN_OTT configuration only. On the other hand Policing (PCC) related test cases were evaluated using UNI-MC-LTE configuration and eMBMS (eMBMS) used MULTI-MC-LTE configuration.

The following tables collect the test cases grouped by test objective following the structure of the test specification document itself.

Test Id	Test Purpose
CONN-MCPTT/GROUP/PREA/ONDEM/NFC/01	On-demand prearranged MCPTT Group Call (Sections 10.1.1.2.1, 10.1.1.3.1.1 and 10.1.1.4 in)

Test Id	Test Purpose
CONN-MCPTT/GROUP/PREA/ONDEM/NFC/02	On-demand prearranged MCPTT Group Call (Sections 10.1.1.2.1, 10.1.1.3.1.1 and 10.1.1.4 in [9]): Emergency MCPTT Group Call (6.2.8.1.[1-8][13-17] in [9])
CONN-MCPTT/GROUP/PREA/ONDEM/NFC/03	On-demand prearranged MCPTT Group Call (Sections 10.1.1.2.1, 10.1.1.3.1.1 and 10.1.1.4 in [9]): Imminent Peril MCPTT Group Call (6.2.8.1.9-12 in [9])
CONN-MCPTT/GROUP/PREA/ONDEM/NFC/04	On-demand prearranged MCPTT Group Call (Sections 10.1.1.2.1, 10.1.1.3.1.1 and 10.1.1.4 in [9]): Broadcast MCPTT Group Call (6.2.8.2 in [9])
CONN-MCPTT/GROUP/PREA/ONDEM/NFC/05	On-demand prearranged MCPTT Group Call (Sections 10.1.1.2.1, 10.1.1.3.1.1 and 10.1.1.4 in [9] : Upgrade to in-progress emergency or imminent peril (10.1.1.2.1.3, 10.1.2.2.1.4 in [9])
CONN-MCPTT/GROUP/PREA/ONDEM/NFC/06	Termination of an on-demand prearranged MCPTT Group Calls (Sections 10.1.1.2.3.1 and 10.1.1.3.3.1 in [9])
CONN-MCPTT/GROUP/PREA/PRE/NFC/01	Prearranged MCPTT Group Call using pre-established session (Sections 10.1.1.2.2, 10.1.1.3.1.2 and 10.1.1.4 in [9]
CONN-MCPTT/GROUP/PREA/PRE/NFC/02	Termination of a prearranged MCPTT Group Call using pre-established session (Sections 10.1.1.2.3.2 and 10.1.1.3.3.2 in [9])
CONN-MCPTT/GROUP/CHAT/ONDEM/NFC/01	On-demand MCPTT Chat Group Call establishment (Sections 10.1.2.2.1.1, 10.1.2.3.1.1, 10.1.2.3.1.3 and 10.1.2.4.1.1 in [9])
CONN-MCPTT/GROUP/CHAT/ONDEM/NFC/02	Ongoing on-demand MCPTT Chat Group Call upgraded to emergency call (Sections 10.1.2.2.1.4, 10.1.2.2.1.2, 10.1.2.3.1.2, 10.1.2.3.1.4 and 10.1.2.4.1.2 in [9])
CONN-MCPTT/GROUP/CHAT/ONDEM/NFC/03	Ongoing on-demand MCPTT Chat Group Call upgraded to imminent peril (Sections 10.1.2.2.1.4, 10.1.2.2.1.2, 10.1.2.3.1.2, 10.1.2.3.1.4 and 10.1.2.4.1.3 in [9])
CONN-MCPTT/GROUP/CHAT/ONDEM/NFC/04	Cancellation of the in-progress emergency condition of an on-demand MCPTT Chat Group Call (Sections 10.1.2.2.1.3, 10.1.2.2.1.2, 10.1.2.3.1.2, 10.1.2.3.1.4 and 10.1.2.4.1.2 in [9])
CONN-MCPTT/GROUP/CHAT/ONDEM/NFC/05	Cancellation of the in-progress imminent peril condition of an on-demand MCPTT Chat Group Call (Sections 10.1.2.2.1.5, 10.1.2.2.1.2, 10.1.2.3.1.2, 10.1.2.3.1.4 and 10.1.2.4.1.3 in [9])
CONN-MCPTT/GROUP/CHAT/PRE/NFC/01	MCPTT Chat Group Call establishment within a pre-established session (Sections 10.1.2.2.2, 10.1.2.2.1.6, 10.1.2.3.2.1, 10.1.2.3.2.2 and 10.1.2.4.1.1 in [9])
CONN-MCPTT/PRIV/AUTO/ONDEM/WFC/NFC/01	On-demand private MCPTT call with floor control (Section 11.1.1.2.1 in [9]) and automatic commencement mode, see [31])
CONN-MCPTT/PRIV/MAN/ONDEM/WFC/NFC/01	On-demand private MCPTT call with floor control manual mode (Section 11.1.1.2.1 in [9]) and manual commencement mode, see [31])
CONN-MCPTT/PRIV/AUTO/PRE/WFC/NFC/01	Pre-established private MCPTT call with floor control (Section 11.1.1.2.1 in [9]) and automatic commencement mode, see [31])
CONN-MCPTT/PRIV/MAN/PRE/WFC/NFC/01	Pre-established private MCPTT call with floor control manual mode (Section 11.1.1.2.1 in [9]) and manual commencement mode, see [31])
CONN-MCPTT/PRIV/AUTO/ONDEM/WOFC/01	On-demand private MCPTT call without floor control (Section 11.1.1.2.1 in [9]) and automatic commencement mode, see [31])
CONN-MCPTT/PRIV/MAN/ONDEM/WOFC/01	On-demand private MCPTT call without floor control manual mode (Section 11.1.1.2.1 in [9]) and manual commencement mode, see [31])
CONN-MCPTT/PRIV/AUTO/PRE/WOFC/01	Pre-established private MCPTT call without floor control (Section 11.1.1.2.1 in [9]) and automatic commencement mode, see [31])
CONN-MCPTT/PRIV/MAN/PRE/WOFC/01	Pre-established private MCPTT call without floor control manual mode (Section 11.1.1.2.1 in [9]) and manual commencement mode, see [31])
CONN-MCPTT/ONN/FIRST/MANUAL/ONDEM/WFC/NFC/01	MCPTT User initiates an on-demand first-to-answer MCPTT call with floor control (Sections 11.1.1.2.1, 11.1.1.3.1.1 and 11.1.1.4 in [9])
CONN-MCPTT/ONN/FIRST/MANUAL/ONDEM/WOFC/NFC/01	MCPTT User initiates an on-demand first-to-answer MCPTT call without floor control (Section 11.1.2 in [9])

Test Id	Test Purpose
CONN-MCPTT/ONN/FIRST/MANUAL/PRE/WFC/NFC/01	MCPTT User initiates an on-demand first-to-answer MCPTT call with floor control using pre-established sessions (Sections 11.1.1.2.2, 11.1.1.3.1.2, 11.1.3.2.2 and 11.1.1.4 in [9] and [30])
CONN-MCPTT/ONN/FIRST/MANUAL/PRE/WOFC/01	MCPTT User initiates a pre-established first-to-answer MCPTT call in manual commencement mode without floor control
CONN-MCPTT/ONN/CALLBACK/SETUP/01	MCPTT User setups a private-call callback (Sections 11.1.1.2.1, 11.1.1.3.1.1 and 11.1.1.4 in [9])
CONN-MCPTT/ONN/CALLBACK/CANCEL/01	MCPTT User cancels a private-call callback (Section 11.1.2 in [9])
CONN-MCPTT/ONN/CALLBACK/FULFIL/01	MCPTT User fulfils a private-call callback
CONN-MCPTT/ONN/AMBIENT/ONDEM/LOCAL/01	MCPTT User setups locally an on-demand ambient listening call (Sections 11.1.6.2.1.1, 11.1.6.3 and 11.1.6.4 in [9])
CONN-MCPTT/ONN/AMBIENT/ONDEM/LOCAL/02	MCPTT User releases locally an on-demand ambient listening call (Section 11.1.6.2.1.3 in [9])
CONN-MCPTT/ONN/AMBIENT/PRE/LOCAL/01	MCPTT User setups locally an ambient listening call using pre-established session (Section 11.1.6.2.2 in [\ref{nr:3gpp-ts-23379}])
CONN-MCPTT/ONN/AMBIENT/PRE/LOCAL/02	MCPTT User releases locally an ambient listening call using pre-established session (Section 11.1.6.2.2.3 in [9])
CONN-MCPTT/ONN/AMBIENT/ONDEM/REMOTE/01	MCPTT User setups remotely an on-demand ambient listening call (Section 11.1.6.2.1.1 in [9])
CONN-MCPTT/ONN/AMBIENT/ONDEM/REMOTE/02	MCPTT User releases remotely an on-demand ambient listening call (Section 11.1.6.2.1.3 in [9])
CONN-MCPTT/ONN/AMBIENT/PRE/REMOTE/01	MCPTT User setups remotely an ambient listening call using pre-established session
CONN-MCPTT/ONN/AMBIENT/PRE/REMOTE/02	MCPTT User releases remotely an ambient listening call using pre-established session
CONN-MCPTT/ONN/GROUPCHANGE/01	Remote change of selected group (Section 10.1.4 in [9])
CONN-MCDATA/O2O/STANDALONE/SDS/SIP/01	One-to-one standalone SDS over SIP
CONN-MCDATA/O2O/STANDALONE/SDS/MSRP/01	One-to-one standalone SDS over media plane (MSRP)
CONN-MCDATA/O2O/SESSION/SDS/MSRP/01	One-to-one SDS session
CONN-MCDATA/GROUP/STANDALONE/SDS/SIP/01	Group standalone SDS over SIP
CONN-MCDATA/GROUP/STANDALONE/SDS/MSRP/01	Group standalone SDS over media plane (MSRP)
CONN-MCDATA/GROUP/SESSION/SDS/MSRP/01	Group SDS session
CONN-MCDATA/O2O/FD/HTTP/01	One-to-one FD using HTTP
CONN-MCDATA/GROUP/FD/HTTP/01	Group FD using HTTP
CONN-MCDATA/O2O/FD/MSRP/01	One-to-one FD using media plane (MSRP)
CONN-MCDATA/GROUP/FD/MSRP/01	Group FD using media plane (MSRP)
CONN-MCDATA/DISNOT/SDS/01	Standalone SDS with delivered and read notification
CONN-MCDATA/DISNOT/SDS/02	Group standalone SDS with delivered and read notification
CONN-MCDATA/DISNOT/FD/01	One-to-one FD using HTTP with file download completed notification
CONN-MCDATA/DISNOT/FD/02	Group FD using HTTP with file download completed notification
CONN-MCDATA/NET/FD/01	Network triggered FD notifications

Table 15. Test Group for the Connectivity (CONN) objective

Test Id	Test Purpose
FC/BASIC/01	Basic FC functionality (Subclause 6 in 3GPP TS 24.380 [10])
FC/BASIC/02	Basic FC functionality. Effect of Priorities (following A.3.5 example in 3GPP TS 24.380 [10]

Table 16. Test Group for the Floor Controlling (FC) objective

Test Id	Test Purpose
REGAUTH/IDMSAUTH/01	MCPTT Client authentication and tokens retrieval using IdMS

Test Id	Test Purpose
	3GPP TS 24.482 [12]
REGAUTH/3PRTYREG/REGISTER/01	MCPTT Client registration using 3rd party register (Subclauses 7.2.1 and 7.3.2 in 3GPP TS 24.379 [9])
REGAUTH/PUBLISH/REGISTER/01	MCPTT Client registration using SIP PUBLISH (Subclauses 7.2.2 and 7.3.3 in 3GPP TS 24.379 [9])

Table 17. Test Group for the Registration and Authorization (REGAUTH) objective

Test Id	Test Purpose
PCC/BEARERSETUP/01	Unicast MC Bearer Setup by SIP Core/IMS (Sections 4.4.1 and 4.4.2 in [21])
PCC/BEARERSETUP/02	Unicast MC Bearer Setup by MCPTT Participating AS (Sections 4.4.1 and 4.4.2 in [21])
PCC/BEARERUPDATE/01	Unicast MC Bearer Update by SIP Core/IMS due to a change in the Call characteristics
PCC/BEARERUPDATE/02	Unicast MC Bearer Update by MCPTT Participating AS due to a change in the Call characteristics
PCC/BEARERSETUP/03	Unicast MC Bearer Setup by SIP Core/IMS using pre-established sessions (Sections 4.4.1 and 4.4.2 in [21])
PCC/BEARERSETUP/04	Unicast MC Bearer Setup by MCPTT Participating AS using pre-established sessions (Sections 4.4.1 and 4.4.2 in [21])

Table 18. Test Group for the Policing (PCC) objective

Test Id	Test Purpose
EMBMS/ACTIVATEBEARER/WPRETMGI/01	Use of dynamically established MBMS bearers in prearranged MCPTT group calls with pre-allocated TMGIs (Subclauses 5.2.1 and 5.3.2 in 3GPP TS 29.468 [23])
EMBMS/ACTIVATEBEARER/WOPRETMGI/01	Use of dynamically established MBMS bearers in prearranged MCPTT group calls without pre-allocated TMGIs
EMBMS/PREBEARER/WPRETMGI/01	Use of pre-established MBMS bearers in prearranged group calls with pre-allocated TMGIs
EMBMS/PREBEARER/WOPRETMGI/01	Use of pre-established MBMS bearers in prearranged group calls without pre-allocated TMGIs
EMBMS/MODIFYBEARER/01	Modification of MBMS bearers upon reception of emergency upgrade request
EMBMS/DEACTIVBEARER/WTMGIDEA/01	Deactivation of MBMS bearers after termination of a prearranged MCPTT group call with TMGI deallocation
EMBMS/DEACTIVBEARER/WOTMGIDEA/01	Deactivation of MBMS bearers after termination of a prearranged MCPTT group call without TMGI deallocation
EMBMS/SWITCHTOUNITMGIEXP/01	Switching to unicast bearer after TMGI expiration

Table 19. Test Group for the eMBMS (eMBMS) objective

Test Id	Test Purpose
AFFIL/DET/01	Determining self affiliation (Subclauses 9.2.1.3 and 9.2.2.2.4 in 3GPP TS 24.379 [9])
AFFIL/DET/02	Determining affiliation status of another user (Subclauses 9.2.1.3 and 9.2.2.2.4 in 3GPP TS 24.379 [9])
AFFIL/CHANGE/01	Affiliation status change triggered by the MCPTT User itself (Subclauses 9.2.1.2 and 9.2.2.2.3 in 3GPP TS 24.379 [9])
AFFIL/CHANGE/02	Affiliation status change triggered by another MCPTT User in mandatory mode (Subclauses 9.2.1.2, 9.2.2.3.3 in 3GPP TS 24.379 [9])
AFFIL/CHANGE/03	Affiliation status change triggered by another MCPTT User in

Test Id	Test Purpose
	negotiated mode (Subclauses 9.2.1.4 and 9.2.1.5 in 3GPP TS 24.379 [9])

Table 20. Test Group for the Affiliation (AFFIL) objective

Test Id	Test Purpose
LOC/3PRTYREG/CONFIG/01	MCPTT Client Configuration upon 3rd party register (Subclauses 13.2.2 and 13.3.2 in 3GPP TS 24.379 [9])
LOC/REQUEST/01	Request for Location Report to the MCPTT Client (Subclauses 13.2.3 and 13.3.3 in 3GPP TS 24.379 [9])
LOC/SUBMISSION/01	MCPTT Client Sends location upon trigger (Section 13.3.4 in 3GPP TS 24.379 [9])

Table 21. Test Group for the Location (LOC) objective

Test Id	Test Purpose
CSC-CMS/UECONF/UE/01	Subscription and UE configuration document retrieval from the MC UE (Sections 6.3.3 and 6.3.13 -specifically 6.3.13.2.2a and 6.3.13.3.2.3f- in [14]), OMA XDM mechanisms and procedures in [29])
CSC-CMS/UPROCONF/UE/01	Subscription and user profile configuration document retrieval from the MC UE
CSC-CMS/SERVCONF/UE/01	Subscription and service configuration document retrieval from the MC UE
CSC-CMS/SERVCONF/MCSSERV/01	Subscription and service configuration document retrieval from the MCS server
CSC-GMS/GROUP/UE/01	Subscription and group document retrieval from the MC UE
CSC-GMS/GROUP/MCSSERV/01	Subscription and group document retrieval from the MCS Server
CSC/MULTIPLESUBS/GROUP/UE/01	Subscription and retrieval of multiple documents from the CMS using subscription proxy

Table 22. Test Group for the OAM Procedures (CSC) objective

Test Id	Test Purpose
SEC/KEYMDOWNLOAD/WPROXY/01	Key material download from KMS to MCPTT client (CSC-8) with proxy
SEC/KEYMDOWNLOAD/WPROXY/02	Key material download from KMS to MCPTT server (CSC-9) with proxy
SEC/KEYMDOWNLOAD/WPROXY/03	Key material download from KMS to MCPTT GMS (CSC-10) with proxy
SEC/KEYMDOWNLOAD/WOPROXY/01	Key material download from KMS to MCPTT client (CSC-8) without proxy
SEC/KEYMDOWNLOAD/WOPROXY/02	Key material download from KMS to MCPTT server (CSC-9) without proxy
SEC/KEYMDOWNLOAD/WOPROXY/03	Key material download from KMS to MCPTT GMS (CSC-10) without proxy
SEC/KEYDIST/CSK/01	Key management from MC client to MC server (CSK upload)
SEC/KEYDIST/GMK/01	Key management for group communications (GMK)
SEC/KEYDIST/MUSIK/01	Key management from MC server to MC client (Key download MuSiK)
SEC/ENCRYPTION/PRIVATE/01	Encryption of MCPTT private calls (use of derived encryption keys from PCK for the audio and CSK for floor control and RTCP reports)
SEC/ENCRYPTION/GROUP/01	Encryption of MCPTT group calls (use of derived encryption keys from GMK for the audio and CSK for floor control and RTCP reports)
SEC/ENCRYPTION/GROUPEMBMS/01	Encryption of MCPTT group calls using eMBMS (use of derived

Test Id	Test Purpose
	encryption keys from MuSIK for the floor control and MSCCK for eMBMS control)
SEC/XMLENCRYPT/PRIVATE/01	XML contents encryption in MCPTT private calls (mcptt-info and resource-lists)
SEC/XMLENCRYPT/GROUP/01	XML contents encryption in MCPTT group calls (mcptt-info)
SEC/XMLENCRYPT/AFFIL/01	XML contents encryption in affiliation procedure
SEC/XMLENCRYPT/LOC/01	XML contents encryption in location procedure

Table 23. Test Group for the Security (SEC) objective

9 Interoperability Results

9.1 Overall Results

During the Plugtests event, a total of 300 Test Sessions were run: that is, 300 different combinations based on different configurations in Test Scope: MCPTT Client, MCPTT Server (Participating and Controlling), MCData Client, MCData Server, MCVideo Client, MCVideo Server, UE, eNB and IMS/SIP Core were tested for interoperability. Overall, 2155 individual test cases were run and reported interoperability 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. The non-executed Test Cases were marked “NA” (Not Applicable) during the Test Session, to indicate that at least one of the EUTs involved in the Test Session did not support the feature in scope.

Interoperability		Totals
OK	**NO**	**Run**
2003 (92.9%)	152 (7.1%)	2155

Table 24. Overall Results

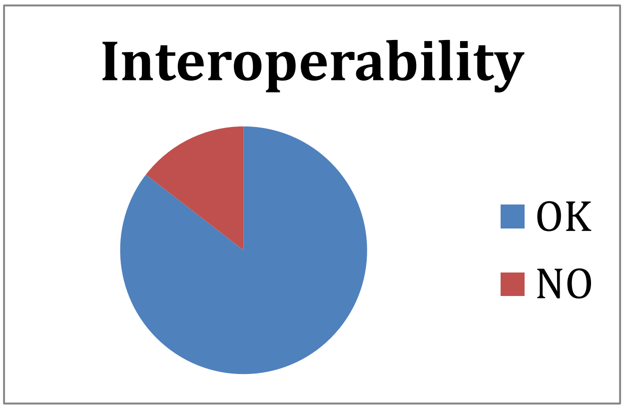

Figure 13. Overall results (%)

A overall interoperability success rate of 92.9% was achieved, which indicates a very high 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 below provides the results for each test configuration in the scope of the Plugtests event.

Configurations	Interoperability		Execution Rate	
	OK	NO	NA	Run
PreTest_CONFIG 1	498 (92.9%)	38 (7.1%)	2358 (81.5%)	536 (18.5%)
PreTest_CONFIG 2_MBMS	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
PreTest_CONFIG 3	61 (100.0%)	0 (0.0%)	134 (68.7%)	61 (31.3%)

Configurations	Interoperability		Execution Rate	
	OK	NO	NA	Run
Main_CONFIG 1	1100 (91.9%)	97 (8.1%)	3838 (76.2%)	1158 (23.5%)
Main_CONFIG 2_eMBMS	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
Main_CONFIG 3	17 (89.5%)	2 (10.5%)	0 (0.0%)	19 (100.0%)
Main_CONFIG 4	104 (88.9%)	13 (11.1%)	520 (81.6%)	120 (18.8%)
Main_CONFIG 5	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
Main_CONFIG 6	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
Pretest_CONFIG 4 MBMS OTT	86 (98.9%)	1 (1.1%)	0 (0.0%)	86 (100.0%)
Main_CONFIG 8 MBMS OTT	105 (99.1%)	1 (0.9%)	29 (21.5%)	98 (77.2%)
Main_CONFIG 9 Audio Testing	10 (100.0%)	0 (0.0%)	0 (0.0%)	10 (100.0%)
Main_CONFIG 10 Audio Testing	4 (100.0%)	0 (0.0%)	1 (20.0%)	4 (80.0%)
Main_CONFIG 11	8 (100.0%)	0 (0.0%)	7 (46.7%)	8 (53.3%)
Main_CONFIG 12	7 (100.0%)	0 (0.0%)	0 (0.0%)	7 (100.0%)
Main_CONFIG 13	3 (100.0%)	0 (0.0%)	0 (0.0%)	3 (100.0%)

Table 25. Results per Test Configuration

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

9.3 Results per Test Case

The table below provides the results for each test case in the scope of the Plugtests event.

Test Cases	Interoperability		Execution Rate	
	OK	NO	NA	Run
7.2.1	102 (91.1%)	10 (8.9%)	36 (24.3%)	0 (0.0%)
7.2.2	54 (98.2%)	1 (1.8%)	51 (48.1%)	0 (0.0%)
7.2.3	46 (97.9%)	1 (2.1%)	54 (53.5%)	0 (0.0%)
7.2.4	35 (97.2%)	1 (2.8%)	63 (63.6%)	0 (0.0%)
7.2.5	11 (78.6%)	3 (21.4%)	83 (85.6%)	0 (0.0%)
7.2.6	81 (97.6%)	2 (2.4%)	40 (32.5%)	0 (0.0%)
7.2.7	5 (100.0%)	0 (0.0%)	83 (94.3%)	0 (0.0%)
7.2.8	3 (100.0%)	0 (0.0%)	83 (96.5%)	0 (0.0%)
7.2.9	82 (93.2%)	6 (6.8%)	41 (31.8%)	0 (0.0%)
7.2.10	9 (81.8%)	2 (18.2%)	76 (87.4%)	0 (0.0%)
7.2.11	6 (85.7%)	1 (14.3%)	79 (91.9%)	0 (0.0%)
7.2.12	6 (100.0%)	0 (0.0%)	78 (92.9%)	0 (0.0%)
7.2.13	4 (100.0%)	0 (0.0%)	81 (95.3%)	0 (0.0%)
7.2.14	0 (0.0%)	0 (0.0%)	85 (100.0%)	0 (0.0%)
7.2.15	82 (92.1%)	7 (7.9%)	37 (29.4%)	0 (0.0%)
7.2.16	80 (94.1%)	5 (5.9%)	38 (30.9%)	0 (0.0%)
7.2.17	5 (100.0%)	0 (0.0%)	83 (94.3%)	0 (0.0%)
7.2.18	1 (100.0%)	0 (0.0%)	83 (98.8%)	0 (0.0%)
7.2.19	57 (95.0%)	3 (5.0%)	52 (46.4%)	0 (0.0%)
7.2.20	64 (100.0%)	0 (0.0%)	33 (34.0%)	0 (0.0%)
7.2.21	1 (100.0%)	0 (0.0%)	83 (98.8%)	0 (0.0%)
7.2.22	1 (100.0%)	0 (0.0%)	83 (98.8%)	0 (0.0%)
7.2.23	9 (90.0%)	1 (10.0%)	70 (87.5%)	0 (0.0%)
7.2.24	8 (88.9%)	1 (11.1%)	70 (88.6%)	0 (0.0%)
7.2.25	4 (100.0%)	0 (0.0%)	76 (95.0%)	0 (0.0%)

Test Cases	Interoperability		Execution Rate	
	OK	NO	NA	Run
7.2.26	2 (100.0%)	0 (0.0%)	81 (97.6%)	0 (0.0%)
7.2.27	6 (100.0%)	0 (0.0%)	72 (92.3%)	0 (0.0%)
7.2.28	5 (100.0%)	0 (0.0%)	72 (93.5%)	0 (0.0%)
7.2.29	3 (100.0%)	0 (0.0%)	72 (96.0%)	0 (0.0%)
7.2.30	11 (100.0%)	0 (0.0%)	67 (85.9%)	0 (0.0%)
7.2.31	9 (100.0%)	0 (0.0%)	69 (88.5%)	0 (0.0%)
7.2.32	1 (100.0%)	0 (0.0%)	81 (98.8%)	0 (0.0%)
7.2.33	1 (100.0%)	0 (0.0%)	81 (98.8%)	0 (0.0%)
7.2.34	13 (100.0%)	0 (0.0%)	65 (83.3%)	0 (0.0%)
7.2.35	11 (100.0%)	0 (0.0%)	66 (85.7%)	0 (0.0%)
7.2.36	0 (0.0%)	0 (0.0%)	82 (100.0%)	0 (0.0%)
7.2.37	0 (0.0%)	0 (0.0%)	82 (100.0%)	0 (0.0%)
7.2.38	0 (0.0%)	0 (0.0%)	81 (100.0%)	0 (0.0%)
7.2.39	25 (73.5%)	9 (26.5%)	56 (62.2%)	0 (0.0%)
7.2.40	1 (100.0%)	0 (0.0%)	81 (98.8%)	0 (0.0%)
7.2.41	1 (100.0%)	0 (0.0%)	80 (98.8%)	0 (0.0%)
7.2.42	15 (88.2%)	2 (11.8%)	61 (78.2%)	0 (0.0%)
7.2.43	1 (100.0%)	0 (0.0%)	81 (98.8%)	0 (0.0%)
7.2.44	0 (0.0%)	0 (0.0%)	81 (100.0%)	0 (0.0%)
7.2.45	4 (100.0%)	0 (0.0%)	76 (95.0%)	0 (0.0%)
7.2.46	0 (0.0%)	0 (0.0%)	79 (100.0%)	0 (0.0%)
7.2.47	0 (0.0%)	0 (0.0%)	81 (100.0%)	0 (0.0%)
7.2.48	0 (0.0%)	0 (0.0%)	81 (100.0%)	0 (0.0%)
7.2.49	3 (75.0%)	1 (25.0%)	71 (94.7%)	0 (0.0%)
7.2.50	2 (50.0%)	2 (50.0%)	70 (94.6%)	0 (0.0%)
7.2.51	0 (0.0%)	0 (0.0%)	81 (100.0%)	0 (0.0%)
7.2.52	0 (0.0%)	0 (0.0%)	81 (100.0%)	0 (0.0%)
7.2.53	0 (0.0%)	0 (0.0%)	81 (100.0%)	0 (0.0%)
7.2.54	4 (57.1%)	3 (42.9%)	72 (91.1%)	6 (7.8%)
7.2.55	11 (91.7%)	1 (8.3%)	67 (84.8%)	10 (13.0%)
7.2.56	3 (75.0%)	1 (25.0%)	73 (94.8%)	4 (5.3%)
7.2.57	1 (100.0%)	0 (0.0%)	75 (98.7%)	1 (1.3%)
7.3.1	103 (90.4%)	11 (9.6%)	22 (16.2%)	0 (0.0%)
7.3.2	36 (76.6%)	11 (23.4%)	43 (47.8%)	0 (0.0%)
7.4.1	51 (82.3%)	11 (17.7%)	50 (44.6%)	0 (0.0%)
7.4.2	193 (97.0%)	6 (3.0%)	10 (4.8%)	0 (0.0%)
7.4.3	81 (94.2%)	5 (5.8%)	42 (32.8%)	0 (0.0%)
7.5.1	2 (100.0%)	0 (0.0%)	79 (97.5%)	0 (0.0%)
7.5.2	7 (100.0%)	0 (0.0%)	76 (91.6%)	0 (0.0%)
7.5.3	1 (100.0%)	0 (0.0%)	80 (98.8%)	0 (0.0%)
7.5.4	6 (100.0%)	0 (0.0%)	77 (92.8%)	0 (0.0%)
7.6.2	11 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
7.6.3	9 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
7.6.4	10 (100.0%)	0 (0.0%)	2 (16.7%)	0 (0.0%)
7.6.5	7 (100.0%)	0 (0.0%)	2 (22.2%)	0 (0.0%)
7.6.6	7 (87.5%)	1 (12.5%)	1 (11.1%)	0 (0.0%)

Test Cases	Interoperability		Execution Rate	
	OK	NO	NA	Run
7.6.7	15 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
7.6.8	11 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
7.6.9	0 (0.0%)	0 (0.0%)	2 (100.0%)	0 (0.0%)
7.7.1	147 (93.0%)	11 (7.0%)	10 (6.0%)	0 (0.0%)
7.7.2	32 (91.4%)	3 (8.6%)	58 (62.4%)	0 (0.0%)
7.7.3	101 (86.3%)	16 (13.7%)	22 (15.8%)	0 (0.0%)
7.7.4	11 (100.0%)	0 (0.0%)	70 (86.4%)	0 (0.0%)
7.7.5	7 (100.0%)	0 (0.0%)	78 (91.8%)	0 (0.0%)
7.8.1	41 (89.1%)	5 (10.9%)	48 (51.1%)	0 (0.0%)
7.8.2	13 (100.0%)	0 (0.0%)	64 (83.1%)	0 (0.0%)
7.8.3	23 (92.0%)	2 (8.0%)	55 (68.8%)	0 (0.0%)
7.9.1	3 (100.0%)	0 (0.0%)	74 (96.1%)	0 (0.0%)
7.9.2	3 (75.0%)	1 (25.0%)	75 (94.9%)	0 (0.0%)
7.9.3	2 (66.7%)	1 (33.3%)	79 (96.3%)	0 (0.0%)
7.9.4	10 (100.0%)	0 (0.0%)	76 (88.4%)	0 (0.0%)
7.9.5	6 (100.0%)	0 (0.0%)	77 (92.8%)	0 (0.0%)
7.9.6	11 (100.0%)	0 (0.0%)	76 (87.4%)	0 (0.0%)
7.9.7	7 (77.8%)	2 (22.2%)	76 (89.4%)	0 (0.0%)
7.10.1	0 (0.0%)	1 (100.0%)	82 (98.8%)	0 (0.0%)
7.10.2	0 (0.0%)	0 (0.0%)	82 (100.0%)	0 (0.0%)
7.10.3	0 (0.0%)	0 (0.0%)	82 (100.0%)	0 (0.0%)
7.10.4	1 (100.0%)	0 (0.0%)	82 (98.8%)	0 (0.0%)
7.10.5	0 (0.0%)	1 (100.0%)	82 (98.8%)	0 (0.0%)
7.10.6	0 (0.0%)	0 (0.0%)	82 (100.0%)	0 (0.0%)
7.10.7	0 (0.0%)	0 (0.0%)	82 (100.0%)	0 (0.0%)
7.10.8	0 (0.0%)	0 (0.0%)	82 (100.0%)	0 (0.0%)
7.10.9	0 (0.0%)	0 (0.0%)	82 (100.0%)	0 (0.0%)
7.10.10	2 (100.0%)	0 (0.0%)	82 (97.6%)	0 (0.0%)
7.10.11	1 (100.0%)	0 (0.0%)	82 (98.8%)	0 (0.0%)
7.10.12	0 (0.0%)	0 (0.0%)	82 (100.0%)	0 (0.0%)
7.10.13	0 (0.0%)	0 (0.0%)	82 (100.0%)	0 (0.0%)
7.10.14	0 (0.0%)	0 (0.0%)	82 (100.0%)	0 (0.0%)
7.10.15	0 (0.0%)	0 (0.0%)	82 (100.0%)	0 (0.0%)
7.10.16	0 (0.0%)	0 (0.0%)	81 (100.0%)	0 (0.0%)
7.10.17	0 (0.0%)	0 (0.0%)	82 (100.0%)	0 (0.0%)
8.2.1	23 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
8.2.2	22 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
8.2.3	25 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
8.2.4	22 (100.0%)	0 (0.0%)	1 (4.3%)	0 (0.0%)
8.2.5	12 (100.0%)	0 (0.0%)	1 (7.7%)	0 (0.0%)
8.2.6	14 (100.0%)	0 (0.0%)	1 (6.7%)	0 (0.0%)
8.2.7	0 (0.0%)	0 (0.0%)	3 (100.0%)	0 (0.0%)
8.2.8	1 (100.0%)	0 (0.0%)	2 (66.7%)	0 (0.0%)
8.2.9	1 (100.0%)	0 (0.0%)	2 (66.7%)	0 (0.0%)
8.2.10	1 (100.0%)	0 (0.0%)	2 (66.7%)	0 (0.0%)
8.2.11	0 (0.0%)	0 (0.0%)	3 (100.0%)	0 (0.0%)

Test Cases	Interoperability		Execution Rate	
	OK	NO	NA	Run
8.2.12	1 (100.0%)	0 (0.0%)	2 (66.7%)	0 (0.0%)
8.2.13	2 (100.0%)	0 (0.0%)	1 (33.3%)	0 (0.0%)
8.2.14	1 (100.0%)	0 (0.0%)	2 (66.7%)	0 (0.0%)
8.2.15	0 (0.0%)	0 (0.0%)	2 (100.0%)	0 (0.0%)
8.2.16	0 (0.0%)	0 (0.0%)	2 (100.0%)	0 (0.0%)
8.2.17	1 (100.0%)	0 (0.0%)	2 (66.7%)	0 (0.0%)
8.2.18	1 (50.0%)	1 (50.0%)	1 (33.3%)	0 (0.0%)
8.2.19	2 (100.0%)	0 (0.0%)	2 (50.0%)	0 (0.0%)
Audio Quality Uplink	6 (100.0%)	0 (0.0%)	1 (14.3%)	6 (85.7%)
Audio Quality Downlink	8 (100.0%)	0 (0.0%)	0 (0.0%)	8 (100.0%)

Table 26. Results per Test Case

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 MCPTT 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 TS approved in December 2017 (mostly 14.4.0) were considered for the second Plugtests event and some fields may have changed or have been already solved.

The 2nd MCPTT 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 Standards issues

10.1.1 MCPTT Administrator designation and checks

Not only on TS 24.484, but on other MCPTT related standards, the "MCPTT Administrator" is mentioned several times. In no single document is specified how this special MCPTT User is identified or distinguished from other regular MCPTT users. For CMS in particular, it is important to clarify this point, as this is the only user that can provision/manage configuration documents in this server. The checking mechanism should be specified. It is suggested to check the MCPTT ID of the access token against a configured value in the CMS.

10.1.2 MO and XML Document relationship

It is mentioned in TS 24.484, Figure 4.2.2-1, that following the bootstrap procedure, UE must download the "MCS UE initial configuration MO" and the "identified default MCS user profile configuration MO". This point is somewhat confusing, because it differs greatly with the wording regarding other CMS documents, where it clearly states that the UE must subscribe to the XML document.

In the case of these two documents (MO's) the TS does not mention the XML format for the documents, but the MO format. And it does not say the UE must subscribe, but simply download those documents. All of this seems to imply that the procedure to follow is wildly different from the regular CMS XML documents.

But, then, reaching section 7.2 of TS 24.484, there is a XML definition for the "MCS UE initial configuration document" (note here the notation change from "MO" to "document").

So, it needs to be clarified whether these two documents must be handled as normal XML CMS documents or have a different handling procedure. Based on what is specified in section 7, these documents should be handled the same way as the rest of the CMS documents. And thus, that figure and accompanying text should be changed to avoid confusion.

10.1.3 CMS Direct Subscription procedure

This procedure wording is causing very different interpretations and may have several technical limitations that can cause serious problems in the implementation phase. First, the direct subscription as defined in 6.3.13.2.2 has several confusing points:

Base URI for the SUBSCRIBE SIP request being equal to the CMSXCAPRootURI. There are enough previous references about CMSXCAPRootURI to somewhat surely assert that this is a HTTP URI like "http://xcap.organization.org/xcap-root". But according to IETF RFC 3261 "SIP elements MAY support Request-URIs with schemes other than "sip" and "sips"", the support for HTTP Req-Uris is somewhat dubious.

The "auid" parameter that must be set to "the appropriate application usage identifying a configuration management document". In XCAP jargon, "application usage [ID]" (AUID), is something like "org.3gpp.mcptt.ue-init-config", which identifies different XCAP applications inside a XCAP Server. This seems to imply that the previous URI must be followed by something like "?auid=org.3gpp.mcptt.ue-init-config". But this two points are repeated the same way to describe the URI's that should be put inside <entry> elements inside the application/resource-lists+xml MIME body, in the subscription proxy procedure described just below. According to IETF RFC 5875, the result of applying these two bullet points should be equal to something along the lines of "org.3gpp.mcdata.service-config/global/service-config.xml".

Both subscription methods seem to be not thoroughly described, but due to subscription proxy method being more widely known, thanks to XCAP Diff and OMA XDM, it seems to be somewhat easier to implement than direct subscription.

It is proposed to use a procedure very similar to the Subscription Proxy for the Direct Subscription use cases: a SIP SUBSCRIBE request with the subscription proxy R-URI, with a application/resource-lists+xml body and a unique <entry> element. It is suggested that this modified Direct Subscription method will be used in case of unauthenticated requests only, that is, MCS Server originated subscriptions and UE (pre-auth) originated subscriptions. For the rest of the UE (post-auth) originated subscriptions we advocate to use Subscription Proxy procedures.

10.1.4 UE-init-conf and UE-conf storage paths and access URIs

It is mentioned on 3GPP TS 24.484 sections 7.2 and 8.2 that "The master MCS UE (initial) configuration document name is assigned by an MCS administrator when the document is created and is stored in the user directory of that MCS administrator." So it is clearly defined where MASTER UE (initial) documents belongs to. These must serve as a template for generating specially targeted configuration documents that eventually are fetched from the correspondent UEs. But the standard does not indicate what URI must the UEs use to access those documents. It is highly improbable for the UEs to be capable of getting the documents from the MCPTT Administrator User's Tree, as this is the only defined path for UE initial document.

For the MCS UE configuration documents, the standard does say that "MCPTT UE configuration documents of a MCPTT user are contained as "XDM collections" in the user's directory of the "Users Tree"" so, at least for this type of document the path to be used for HTTP GET's and subscription is somewhat defined.

We think this should be more thoroughly specified in the standard, and provide a base set of parameters for each configuration document, such as (UE accessible URI, Admin provisionable URI, detailed MASTER -> concrete document transformation procedures). In the current state of the standard, interoperability capacity is very low due to missing details and open interpretation possibilities.

10.1.5 File Extension inclusion in XML values

In several places in the standard it is necessary to reflect documents filenames in different XML elements of the documents. In these cases, the full document file name has to be reflected, such as "mcvideo-userprofile-3shift.xml" or only the filename without the extension "mcvideo-userprofile-3shift".

Examples:

- 3GPP TS 24.484 subclause 8.3.2.7 "The <ProfileName> element is of type "token" and specifies the name of the MCPTT user profile configuration document in the MCPTT user profile XDM collection and corresponds to the "MCPTTUserProfileName" element of subclause 5.2.7B in 3GPP TS 24.483 [4]"
- 3GPP TS 24.484 subclause 9.3.1 "The name of the MCVideo user profile document matches the value of the <ProfileName> element in the MCVideo user profile document."

We advocate for the full filename option in this case, although we hold a little uncertainty about whether this refers to the filename (or document selector in XCAP jargon) or to another kind of "document name.

10.1.6 User profile static name

In 3GPP TS 24.484, all of the user-profile MCS documents have a "Naming Conventions" sections defining static filenames for them like "mcXXX-user-profile".

As we understand user-profile documents, it is possible to have several of them per user, so this unique name definition is somewhat insufficient.

We advocate a change to the specification. The default name for the document shall be the unique name definition with the addition of the profile index value. For instance user-profile-<index-value>.xml or user-profile-1.xml, mcvideo-user-profile-1.xml, etc.

10.1.7 MCX Service Authorization

3GPP TS 33.180 defines two ways of performing MCX Service authorization with the MCX Server, but if we consider the full procedure a UE has to perform to bootstrap from cold start to a full working state within the network, there is a conflict with the REGISTER based workflow.

The REGISTER authorization workflow is based on the idea of including the MCPTT Access Token right in the IMS REGISTER SIP message the UE sends towards the IMS network when contacting it for the first time. But if according to 3GPP TS 24.484, the UE must subscribe to the UE-initial-conf document and the default-user-profile, it has to be already registered in the IMS network, thus rendering the REGISTER workflow unusable.

For the moment PUBLISH Authorization workflow seems to be the only alternative.

10.1.8 MCS Server PSI missing

The MCS Server PSI does not seem to be configured anywhere in the CMS documents. Being a very necessary address to have in order to bootstrap MCPTT functionality in the UE, it seems logical to find it in the UE-initial-conf document, but it is completely missing.

If no other mechanism or impediment is found, we think UE-init-conf document is ideal to add the MCS Server address in order to have all of the network servers addresses specified together.

10.1.9 Misleading typos

There are some types in configuration documents which can be specially misleading or modify significantly the meaning of the sentence. Following are some of them:

- "initial" word misplaced in sentences like "If there is no <mcvideo-UE-id> element in the MCVideo UE configuration document, then by default the MCVideo UE configuration document applies to all MCVideo UEs of the mission critical organization that are not specifically identified in the <mcvideo-UE-id> element of another MCVideo UE initial configuration document of the mission critical organization." This happens in 3GPPP TS 24.484 subclauses 8.2.1, 9.2.1, 9.2.2.7, 10.2.1 and 10.2.2.7 sections.

- The extra point at MCPTT User Profile Document at section 8.3.2.5 of 3GPP TS 24.484. It now says "application/vnd.3gpp.mcptt.-user-profile+xml". That point after the "mcptt" is misleading and probably incorrect, as the other MCX User profile counterparts do not have it.

10.1.10 Duration Data Type in Service Configurations

In 3GPP TS24.484 Section 8.4.2.6 (Page 84) it is stated that:

The elements of "xs: duration" type specified above shall be represented in seconds using the element value: "PT<h>H<m>M<n>S" where <n> represents a valid value in seconds.

NOTE 3: "xs:duration" allows the use of decimal notion for seconds, e.g. 300ms is represented as <PT0.3S>.

If any of the elements of "xs: duration" type specified above contain values that do not conform to the "PT <n>S" structure then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "invalid format for duration"

1. The first sentence is confusing, stating to use the XML Schema's *duration* data type, and also redefining it with a format string of "PT<h>H<m>M<n>S" to prevent the use of "<y>Y<m>M<d>D" between "P" and "T".
2. Also a few lines below, the format string changes to "PT <n>S".

We think that the actual intent behind this text is to define how an amount of time may be specified in the service configuration document. Our proposed way to do that would be to use the XML Schema's duration datatype without modifications as in the other configuration documents.

10.1.11 Nested PrivateCallKMSURI Element in User Profile Configuration

In 3GPP TS 24.484 Section 8.3.2.1 item 8)-i-C-I a *PrivateCallKMSURI* element that contains one or more entry elements is defined. However, in the XSD, the *PrivateCallKMSURI* contains another nested *PrivateCallKMSURI* element, so that for example the following XML snippet is the only way to define a KMS URI with the value "sip:kms1@example.com":

```
<PrivateCallKMSURI>
   <PrivateCallKMSURI>
      <uri-entry>sip:kms1@example.com</uri-entry>
   </PrivateCallKMSURI>
</PrivateCallKMSURI>
```

We hardly see any reason for this nesting, especially, because the only other elements within the outer *PrivateCallKMSURI* element are the *anyExt* and *any* element. To follow the textual description exactly only the following line is needed in the XSD to define the *PrivateCallKMSURI* element:

```
<xs:element name="PrivateCallKMSURI" type="mcpttup:ListEntryType"/>
```

However, this would lead to a similar complex nesting, but at least not using the same name for the nested elements, e.g.:

```
<PrivateCallKMSURI>
   <entry>
      <uri-entry>sip:kms1@example.com</uri-entry>
   </entry>
</PrivateCallKMSURI>
```

So it could be considered a definition like:

```
<xs:element name="PrivateCallKMSURI" type="xs:anyURI"/>
```

Since the *PrivateCallKMSURI* is integrated in the enclosing *PrivateCallList* element using an *anyExt* element there can be an unbounded number of *PrivateCallKMSURI* anyway, which would satisfy the semantics of the textual definition in the standard.

10.1.12 Resource Namespace/Priority in Service Configuration

In 3GPP TS 24.484 Section 8.4.2 it is stated that the *emergency-resource-priority*, *imminent-peril-resource-priority*, and *normal-resource-priority* elements have to contain two elements defined as follows:

a) one <resource-priority-namespace> string element containing a namespace defined in IETF RFC 8101 [20]; and

b) one <resource-priority-priority> string element element containing a priority level in the range specified in IETF RFC 8101 [20];

In RFC 8101 Section 3.1 can be read that:

The mcpttp namespace uses the priority levels listed below from lowest to highest priority.

mcpttp.0 (lowest priority)

mcpttp.1

mcpttp.2

[...]

mcpttp.14

mcpttp.15 (highest priority)

The Namespace Numerical Value is 46.

Analogously, the priorities for the *mcpttq* namespace are defined.

So a priority is the namespace string followed by a period an integer in the range [0,15]. Accordingly, in the XSD the two elements are declared to contain strings:

```
<xs:complexType name="resource-priorityType">
  <xs:sequence>
     <xs:element name="resource-priority-namespace" type="xs:string"/>
     <xs:element name="resource-priority-priority" type="xs:string"/>
     <xs:element name="anyExt" type="mcpttsc:anyExtType" minOccurs="0"/>
     <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>
```

An example would be the following snippet:

```
<emergency-resource-priority>
  <resource-priority-namespace>mcpttp</resource-priority-namespace>
  <resource-priority-priority>mcpttp.14</resource-priority-priority>
</emergency-resource-priority>
```

However, this definition seems to be a little bit confusing, since the name of the namespace is repeated in the *resource-priority-priority* element, where many expect an integer. This would also have the benefit of eliminating redundancy, etc.

We think that this definition could be improved to not only eliminate (potential errors due to) the redundancy (e.g. a namespace of *mcpttp* with a priority of *mcpttq.0* could be defined) but also restrict the priority value. Consider the following XML Schema example snippet in contrast to the *string* data type:

```
<xs:element name="resource-priority-priority">
  <xs:simpleType>
    <xs:restriction base="xs:integer">
      <xs:minInclusive value="0"/>
      <xs:maxInclusive value="15"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
```

10.1.13 On-network and Off-network: May, Shall and how often?

In TS 24.484 Section 7.2.2.1 the contents of the *mcptt-UE-initial-configuration* root element are defined as follows:

The <mcptt-UE- initial-configuration> document:

1) shall include a "domain" attribute;

2) may include a <mcptt-UE-id> element;

3) may include a <name> element;

4) may include a <Default-user-profile> element;

5) may include an <on-network> element;

6) may include an <off-network> element; and

7) may include any other attribute for the purposes of extensibility.

So, the *<mcptt-UE-initial-configuration>* element **may** contain **an** on-network element and **may** also contain **an** off-network element. In contrast, **Section 7.2.2.6** states that *"The <mcptt-UE-initial-configuration> element **shall** contain **one** <on-network> element and **one** <off-network> element."* Additionally, in the XML Schema both elements are nested within a `<xs:choice minOccurs="0" maxOccurs="unbounded">` which means they **may** occur and if they do, they **may** occur more than once.

We would need some clarification on whether presence of an on-network/off-network element is mandatory or not, and in any case, whether a restriction to a single maximum occurrence should be considered.

10.1.14 User Profile Document Name

In TS 24.484 Section 8.3.2.8 it is stated, that *The name of user profile configuration document shall be "user-profile"*, while in Section 8.3.1 the following definition is given: *The name of the MCPTT user profile document matches the value of the <ProfileName> element in the MCPTT user profile document.*

We think the latter naming convention for user profile documents is more practical, since there are certainly more than one in most cases. However, the ProfileName element is not mandatory, so clarification would be needed.

10.1.15 User Profile: PrivateCallURI and PrivateCallProSeUser

The standard states in Section 8.3.2.1 that the *PrivateCallList* element contains a "*<PrivateCallURI> element that contains one or more <entry> elements*" and a "*<PrivateCallProSeUser> element that contains one or more <ProSeUserID-entry> elements*".

In the XSD the *PrivateCallURI* element actually is of type *EntryType* itself and therefore a single entry (named *PrivateCallURI*) and not a list of elements named *entry* of type *EntryType*. Basically the same applies to the *PrivateCallProSeUser* element.

However, because both are nested within a *choice* element with `maxOccurs="unbounded"` they themselves may occur more than once.

10.1.16 Minor but recurring inconsistencies between Structure & Validation chapters and the XSD

In this section a few common types of inconsistencies between the standard text in natural language (mostly the *Structure* and *Validation* sections for **every configuration document** (in 24.484 and 24.481) and the *XML Schema Definition*, are listed with examples. Only one example per type is given.

1. Undefined *any*, *anyExt* and *anyAttribute* elements that are, nevertheless, in the XSD. For example: In the *mcptt-UE-initial-configuration* complex type an *any* and an *anyExt* element are defined without being mentioned in the text. In the textual definintion of the *mcptt-UE-id* neither an *any*, *anyExt*, or *anyAttribute* element are mentioned, but present in the XSD.
2. The *attributeGroup IndexType* is also never mentioned in the text.

10.1.17 Minor inconsistencies between the textual definition and the XSD

In this section a few minor inconsistencies between the standard text in natural language and the *XML Schema Definition*, are listed.

- 7.2.2.3: *mcptt-UE-initial-configuration*: `<xs:element name="HPLM">` maybe should be `<xs:element name="HPLMN">`
- 7.2.2.3: *mcptt-UE-initial-configuration*: `<xs:element name="VPLM">` maybe should be `<xs:element name="VPLMN">`
- The *Instance-ID-URN* attribute in the *mcptt-UE-initial-configuration* complex type is never mentioned to be there in the text.
- 8.3.2.1: *mcptt-user-profile*: The *EmergencyCall* element in the *PrivateCall* element is defined mandatory, but optionally in the XSD.

10.1.18 The *any*, *anyExt*, and *anyAttribute* Discussion

There has been quite some discussion on the pros and cons of using the XML Schema's *any* element, *anyAttribute*, and in this case also the locally defined *anyExtType* (For the sake of readability in the following it will be referred to these elements/attributes casually as "*anys*".). Especially when it comes to the validation of XML documents, there are many different views. We want to point out some examples of noteworthy effects we encountered.

Some noteworthy effects we have encountered so far are:

First, let us have a look at a simple case - here is a snippet:

```
...

    <oxe:supported-services>
        <oxe:service enabler="urn:urn-7:3gpp-service.ims.icsi.mcptt">
            <mcpttgi:mcptt-speech/>
        </oxe:service>
    </oxe:supported-services>

...
```

The error in this example is, that the `<mcpttgi:mcptt-speech/>` element does not belong directly under the `oxe:service` element. According to 3GPP TS 24.481 (Release 14) Section 7.2, this snippet **must** look like this (enclosing the `<mcpttgi:mcptt-speech/>` element within an `<oxe:group-media>` element):

```
...
    <oxe:supported-services>
        <oxe:service enabler="urn:urn-7:3gpp-service.ims.icsi.mcptt">
            <oxe:group-media>
                <mcpttgi:mcptt-speech/>
            </oxe:group-media>
        </oxe:service>
    </oxe:supported-services>
...
```

Nevertheless, using a standard XML Schema validator library the group configuration validates correctly against the associated XSD files.

```
...
    <xs:complexType name="serviceType">
        <xs:sequence minOccurs="0" maxOccurs="unbounded">
            <xs:element name="group-media" type="mediaListType" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="enabler" type="xs:string"/>
        <xs:anyAttribute processContents="lax"/>
    </xs:complexType>
...
```

Another phenomenon that we encountered are "dangling elements" that are present throughout the XSDs. By that we mean elements that in the XSDs are never declared to be used in an enclosing element although the standard defines where they are to be used. This work using *anys*. Here is an example, a snippet from the mcptt-user-profile.xsd:

```
...

<xs:complexType name="PrivateCallListEntryType">
    <xs:choice minOccurs="1" maxOccurs="unbounded">
        <xs:element name="PrivateCallURI" type="mcpttup:EntryType"/>
        <xs:element name="PrivateCallProSeUser" type="mcpttup:ProSeUserEntryType"/>
        <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:choice>
    <xs:attributeGroup ref="mcpttup:IndexType"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>

...

<xs:element name="PrivateCallKMSURI" type="mcpttup:PrivateCallKMSURIEntryType"/>

...

<xs:complexType name="PrivateCallKMSURIEntryType">
    <xs:choice>
        <xs:element name="PrivateCallKMSURI" type="mcpttup:EntryType"/>
        <xs:element name="anyExt" type="mcpttup:anyExtType" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:choice>
    <xs:attributeGroup ref="mcpttup:IndexType"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:complexType>
```

It would, for instance, also have been possible to write the PrivateCallKMSURIEntryType like this:

```
...

<xs:complexType name="PrivateCallListEntryType">
    <xs:choice minOccurs="1" maxOccurs="unbounded">
        <xs:element name="PrivateCallURI" type="mcpttup:EntryType"/>
        <xs:element name="PrivateCallProSeUser" type="mcpttup:ProSeUserEntryType"/>
        <xs:element name="PrivateCallKMSURI" type="mcpttup:PrivateCallKMSURIEntryType"/>
    </xs:choice>
    <xs:attributeGroup ref="mcpttup:IndexType"/>
</xs:complexType>

...
```

However, because of the *anyExt* used to include one of those "dangling elements", we only know what to do with the PrivateCallKMSURI element because in 3GPP TS 24.484, Section 8.3.2.1 it is defined that:

...

The <mcptt-user-profile> document:

...

8) shall include one or more <Common> elements, each of which:

...

d) shall include one <PrivateCall> element. The <PrivateCall> element contains:

...

i) a <PrivateCallList> element that contains:

A) a <PrivateCallURI> element that contains one or more <entry> elements;

B) a <PrivateCallProSeUser> element that contains one or more <ProSeUserID-entry> elements; and

C) an <anyExt> element which may contain:

I) a <PrivateCallKMSURI> element that contains one or more entry> elements; and

...

This is, by the way, the minimal MCPTT user profile, that validates:

```
<?xml version="1.0" encoding="UTF-8"?>
<urn:mcptt-user-profile xmlns:urn="urn:3gpp:mcptt:user-profile:1.0"
    XUI-URI="sip:foo@bar.baz"
    user-profile-index="1" />
```

Although the root element is a complex type with a choice element with minOccurs="1" and some mandatory elements in that choice this is possible. The reason is, that there is an *any* element with minOccurs="0", so one can choose "minimally 1 times 0 any" which results in an empty root element.

10.1.19 MCData notifications

MCData notifications work in the following way:

When a MCData client sends a SDS or FD message, a request to receive notifications can be included. The MCData client who receives the message generates the notifications. The request to receive notifications is included in an additional field in message signalling. The notification messages use their own type and they are also included in the signalling part.

When the server receives a message including a notification request, it must save the Conv ID and Msg ID included in the message. This is necessary because when the server receives a notification it must check that the Conv ID and MSG ID included in it can be correlated to a previous message requesting the notification.

The MCData client must include the ID's from the message which requested the notification in the response. If the server cannot correlate a notification with a previous notification request, it must discard the notification message.

The following problem has been found:

According to 12.2.2.1.4) "if the incoming SIP MESSAGE request does not contain an application/vnd.3gpp.mcdata-info+xml MIME body with a <mcdata-controller-psi> element, shall reject the SIP MESSAGE"

It is stated that originating participating server must check the existence of this tag in the mcdata-info, otherwise it must reject the message.

According to 12.2.1.1 "The MCData client determines the controlling MCData function from the contents of the <mcdata-controller-psi> element contained in the application/vnd.3gpp.mcdata-info+xml MIME body of the incoming SDS or FD message request" and 12.2.1.1 4) shall insert in the SIP MESSAGE request an application/vnd.3gpp.mcdata-info+xml MIME body with an<mcdata-controller-psi> element containing the PSI of the controlling MCData function;

The MCdata client must include this in mcdata-info part, which has previously obtained from the incoming SDS or FD message which includes notification request.

After checking section 9.2.2, which explains how to generate and process SDS messages, the <mcdata-controller-psi> does not appear at any subsection and it does not mandate to include it in SDS messages. Therefore, if we follow this procedure, it does not look possible to generate correct notification messages.

The solution to this issue could be for the server to include its PSI in <mdata-controller-psi> in the initial MESSAGE.

10.1.20 MCVideo Media ID field

A definition for the Media ID field is still missing in TS 24.581. This field is used when the media is multiplexed and is included in some of the message definitions in Section 9.2.4.

10.2 Technical Constraints

During the 1st MCPTT Plugtests some technical constraints regarding how to deal with SBC/NAT. Since during the 2nd Plugtests there have been identified no standardised solutions for some of these constraints, the analysis and constraints are again collected here. Additionally, other common needs for clarification have been gathered (collected as CLARIFICATION) from some participants.

The design of the MCPTT ecosystem as an overlay network on top of SIP/IMS core would allow a seamless and secure, by cyphering specific elements) traversal of information through the SIP/IMS core. The usage of participating ASs, MCPTT specific identities (mcptt-id, mcptt-client-id, etc) and the encoding of most of the relevant information in XML in the body of the SIP messages contributed to this de-coupling while making it possible to deploy MCPTT over different provider’s SIP/IMS Core (i.e. different trust domain).

However, in some cases, 3GPP TSs procedures assume “pure IMS/SIP Core” deployments, with direct e2e IP connectivity between the UE, the IMS/SIP Core and all the ASs for both the signalling and the media streams. Unfortunately, in most of the commercial SIP/IMS deployments (including VoLTE) there exist some kind of Source Border Control-ling or NAT elements that either carry out some B2BUA operation and/or hide/replace original IP:PORT. That would include IMS-ALG/AGW/CGNAT/SBC/BCF/SIP-aware firewalls and DPI elements among others (we will use the term SBC indistinctly for all of them in this Section). The situation is particularly problematic in the MCPTT ecosystem since not only the signalling and audio streams need to reach the different AS but also the Floor Control. Additionally, the MCPTT Floor Control uses RTCP-APP which would be most of the time wrongly processed by currently available SBCs.

Although such kind of SBC elements are not considered as mandatory by 3GPP and the need to consider them in normative work could be argued, the participants agreed that some clarification/agreed procedure would no doubt reduce the deployment and integrations costs. In the following subsections this kind of problems are collected in subclause 10.2.1.

10.2.1 SBC: Contact Header

At least two different situations have been identified.

1) Subclause 4.5 in 3GPP TS 24.379 [5] specifies the use of the contact header to carry the session ID. Most SBCs would however remove the session ID from the contact header and/or replace it. MCPTT client needs anyway the

session ID to release the session according to 3GPP TS 24.379 [5]. Additionally, IETF RFC 3261 [28] states that "The Contact header field provides a SIP or SIPS URI that can be used to contact that specific instance of the UA for subsequent requests" only, so that the usage contact header to manage sessions could be re-visited.

2) Following 1) and according to subclause 6.3.3.1.2, subclause 6.3.2.2.3 and subclause 6.3.2.2.4 MCPTT servers shall include the MCPTT session identity in the Contact header field of SIP INVITE requests and 200 OK final responses. Contact headers can be modified by any SBC in the path between the participating MCPTT server and the MCPTT client. MBMS listening status reports sent by MCPTT clients shall include the MCPTT session identity in the MBMS usage info XML. MCPTT clients cannot learn the correct MCPTT session identity from the Contact header they receive in INVITE requests or 200 OK responses because it has been modified by an intermediate node.

Different alternatives were discussed to overcome both issues (out of standards), collected here for information purposes only:

For 1) A partner proposed considering the Session-ID header (IETF RFC 7989 [29]) as a possible alternative.

For 2) A partner proposed:

- The SBC could preserve just the user part of SIP URI which represents the MCPTT session identity. The client would include this value in the MBMS usage info XML and the MCPTT server could compare this value with the list of identities of ongoing MCPTT sessions, instead of the whole SIP-URI.
- The MCPTT server could include a custom SIP header to be traversed transparently by the SBC set to the MCPTT session identity. The MCPTT client could learn the correct MCPTT session identity from this header.
- The MCPTT server could include an additional tag in MCPTT-INFO body indicating the MCPTT session identity. Again, the MCPTT client could learn the correct MCPTT session identity from this new tag.

10.2.2 SBC: MCPTT-5, Rx

PCC related test cases define either P-CSCF or MCPTT Participating AS triggered Rx-interface operations. The associated Diameter interface with the PCRF demands proper IP-CAN information to be conveyed from the UE to the Application Function (being that the P-CSCF of the AS).

In general purpose IMS/VoLTE deployments if the SBC element is included as IMS-ALG in the P-CSCF it can access that information before the border controlling mechanisms are applied and interface the PCRF with proper IP information.

Proposed solutions include either enforcing transparent modes in the SBC (not always possible due to MCPTT specific headers and SDP media components for media and floor control) or using custom headers.

10.2.3 SBC: Conveying P-Preferred-Service and P-Preferred-Identity

In order to properly map the mcptt_id and IMPU the P-CSCF needs to forward the PAI header with the proper IMPU to the participating (in case different IMPUs -i.e. sip, tel URI, etc- are provided). Similarly the proper P-Asserted-Service needs to arrive at the S-CSCF for proper service routing.

Subclause 10.1.1.2.1.1 in 3GPP TS 24.379 [5] states in step 7) shall include an Accept-Contact header field with the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [30];

Such headers should be properly forwarded by the SIP/IMS Core and any SBC in the path between the UE and the Participating. That would mean either a) trusting the MCPTT Client and the SIP/IMS Core copying the P-Preferred-X headers to P-Asserted-X counterparts in the inner trusted domain or ignoring them at the P-CSCF but properly setting them in any incoming request from MCPTT clients.

In fact, the procedure could be considered as ambiguous in 3GPP TS 24.379 [5]:

In subclause 10.1.1.2.1 for the client step 11) states that "it MAY include a P-Preferred-Identity header field in the SIP INVITE request containing a public user identity as specified in 3GPP TS 24.229 [4]" while in the Participating MCPTT function in subclause 10.1.1.3.1.1 step 2) states that it "SHALL determine the MCPTT ID of the calling user from public user identity in the P-Asserted-Identity header field of the SIP INVITE request…".

10.2.4 CLARIFICATION: Need for Client Authentication in IDMS

Many of the vendors' implementations of IdMS and MCPTT Auth included/required Client Authentication using HTTP Basic Auth.

Regarding TS 33.180 this type of mechanisms is only mentioned a couple of times, for example: "Note that client authentication is REQUIRED for native applications (using PKCE) in order to exchange the authorization code for an access token. Assuming that client secrets are used, the client secret is sent in the HTTP Authorization Header."

But nowhere else in the standard is mentioned the use of client authentication or Basic HTTP Auth mechanisms. It is missing completely from the example just below the aforementioned sentence, in section B.4.2.4. Moreover, most of the implementations require the presence of this Basic HTTP Auth (Authorization header) with a content consisting of user:password coded in Base64. This basic method is not specified in the standard (other than inter-domain auth), although it's specified in RFC 6749.

Adding an additional layer of client/UE authentication to the mix (apart from UE-id registering in the IdMS), would probably not represent any benefit. It really adds up to the UE registration phase, because instead of only provisioning the IdMS with the UE-id, the client secret must be also provisioned back to the UE.

If a discussion finally validates this HTTP Basic mechanism, it would be reasonable to modify the standard to include more details about this, and clarify client authentication procedures.

10.2.5 CLARIFICATION: eMBMS Bearer Preemption. Lack of notification to AS

When bearer preemption occurs, there is no 3GPP related way for the MCE to notify back to the Application Server that a bearer has been preempted. This results in the Application Server to think the bearer is going through, but the client will not receive anything anymore, or at least until the prioritized communication ends.

The MCE should notify such bearer preemption back to the MME that should inform the eMBMS Gateway that could then inform back the BM-SC. Once the BM-SC is aware, it should inform back the AS through the MB2-C interface.

10.2.6 CLARIFICATION: PMCH limitations impacting AS

A PMCH can only contain 28 bearers, so if there are numerous MCX bearers, the MCE needs to be carefully provisioned to allow for such quantity. This is done by creating more PMCH. However, it is also important to think about the capacity of such PMCH since MCPTT, MC Video and MC Data may not have the same capacity requirements. Finally, there can be only 15 PMCH per MBSFN area.

This means that there is a correlation between the number of bearers, the MBSFN area and the capacity of the PMCH. The more bearers, the more PMCH and the less capacity per PMCH. The larger the PMCH are (to accommodate for video), the less PMCH there can be, hence limiting the number of bearers.

Careful provisioning and interaction between BM-SC/MCE and AS is required to optimize the network based on the Mission Critical scenario.

History

Document history		
V0.1.0	03/07/2018	First Draft
V0.2.0	04/07/2018	Adding Plugtests procedure.
V0.3.0	16/07/2018	Adding Plugtests scope
V0.4.0	31/07/2018	Review of whole document with amendments.
V0.5.0	06/08/2018	Correction of figure numbers and formatting.
V1.0.0	20/08/2018	Published document.
V1.1.0	10/10/2018	Minor correction in the observer name