ETSI Plugtests Report V1.0.0 (2017-07)

1st ETSI MCPTT Plugtests
Sophia Antipolis, France
19 – 23 June 2017

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

Contents

Contents 3
Executive Summary 5
1 Introduction 6
2 References 8
3 Abbreviations 10
4 Technical and Project Management 11
4.1 Scope 11
4.2 Timeline 12
4.2.1 Documentation 12
4.2.2 Remote integration & pre-testing 13
4.2.3 Plugtests event 13
4.3 Tools 14
4.3.1 Plugtests event Wiki 14
4.3.2 Test Session Scheduler 14
4.3.3 Test Reporting Tool (TRT) 15
5 Equipment Under Test 16
5.1 MCPTT Application Servers 16
5.2 MCPTT Clients 16
5.3 MCPTT User Equipment 16
5.4 IP Multimedia Subsystem (IMS) 17
5.5 LTE Network Components 17
6 Test Infrastructure 18
6.1 Remote and Local Test Infrastructure 18
7 Test Procedures 19
7.1 Remote Integration & Pre-testing Procedure 19
7.2 Interoperability Testing Procedure 19
8 Test Plan Overview 23
8.1 Introduction 23
8.2 Test configurations 23
8.2.1 Over-The-Top Configuration for On-Network calls (CFG_ONN_OTT-1) 24
8.2.2 Unicast Mission Critical LTE for On-Network calls (CFG_ONN_UNI-MC-LTE-1) 24
8.2.3 Multicast Mission Critical LTE for On-Network calls (CFG_ONN_MULTI-MC-LTE-1) 24
8.2.4 Group of test cases 25
9 Interoperability Results 29
9.1 Overall Results 29
9.2 Results per Test Configuration 29
9.3 Results per Test Case 30
10 Base Specification Validation 34
10.1 MCPTT Standards issues 34
10.1.1 Typo in mpctt-info root element 34
10.1.2 Missing Client ID in 3rd party REGISTER based service authorization 34
10.1.3 Missing reference to Location configuration message upon PUBLISH based authorization 34
10.1.4 Granted SSRC coding 34
10.2 Technical Constraints 35
10.2.1 SBC: Contact Header 36
10.2.2 SBC: MCPTT-5, Rx 36
10.2.3 SBC: Conveying P-Preferred-Service and P-Preferred-Identity 37
10.2.4 CLARIFICATION: Selective (de)affiliation to a specific subset of groups 37
10.2.5 CLARIFICATION: Broadcast calls release mechanism 38
10.2.6 CLARIFICATION: Configuration of MCPTT APN 38
10.2.7 CLARIFICATION: Encoding of <entry> “uri” attribute in REFER in pre-established sessions 38

10.2.8 CLARIFICATION: Inclusion of Answer-Mode header in group calls ... 38
10.2.9 CLARIFICATION: Specific reference to out-of-dialog REFER in the group calls using pre-established session ... 39
10.2.10 CLARIFICATION: CMS Service Configuration Document location ... 39
10.2.11 CLARIFICATION: UE (Init) configuration documents generation ... 39

History ... 40

Executive Summary

After the finalization of the MCPTT standards in 3GPP Release 13, TCCA (the representative body for the global critical communications community) and ETSI agreed to jointly organize the first MCPTT Plugtests event in June 2017. Preparations for the Plugtests event started in January 2017 and after a remote pre-test phase in May 2017, the vendors came together for the Plugtests event from 19-23 June 2017 in Sophia Antipolis at the ETSI headquarter.

In the Plugtests event week about 140 participants from 19 vendors, 7 observers and ETSI were engaged, most of them on-site at Sophia Antipolis, the others supporting remotely from the vendors' premises.

The observers came from government and public safety network operator organizations from Belgium, Finland, France, Norway and the UK.

The following equipment was tested:

- **MCPTT Application Servers** from Airbus, Alea, Genaker, Harris Corporation, Hytera, Nemergent, TASSTA and ZTE.
- **MCPTT Clients** from Airbus, Alea, Armour Communications, Etelm (included in TETRA Base Station), Frequentis (included in Control Room), Funkwerk, Genaker, Harris Corporation, Hytera, Nemergent, Spirent, TASSTA and ZTE.
- **User Equipment** (UE) from Bittium and Funkwerk.
- **LTE network components** Evolved Packet Core (EPC), Evolved Node B (eNB) and Multimedia Broadcast Multicast Service (eMBMS) from Athonet, Ericsson, Expway, Huawei and one2many.
- **IP Multimedia Subsystem** (IMS) from Athonet.

ETSI had developed a test specification with 47 test cases including features like: Group Call, Affiliations and Floor Control.

More than 900 tests were conducted, with a success rate of 85%. 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 final tests of the MCPTT Plugtests event included pre-arranged and chat mode Group Calls, which involved several MCPTT clients, a Control Room, a LTE cab radio and a TETRA radio.

The **highlight** of the Plugtests event were the final MCPTT tests which included pre-arranged and chat mode Group Calls. The group calls were set up on an MCPTT Application Server and the MCPTT Clients joined the call. In the end the Group Call involved several MCPTT clients, a Control Room, a LTE cab radio and a TETRA radio.

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

The next MCPTT Plugtests event is planned for Q2 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 supports mission-critical communications.

Although the PMR market shows no signs of slowing, mission-critical broadband LTE 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. Planned 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 are planned for Release 14 and later.

After the finalization of the MCPTT standards in Release 13 at the end of 2016, TCCA (the representative body for the global critical communications community) and ETSI jointly approached vendors of MCPTT systems and MCPTT components. It was agreed to set up the first MCPTT Plugtests event in June 2017.

Preparations for the Plugtests event started in January 2017 with the registrations of vendors and observers. During bi-weekly conference calls from January to June 2017 the setup of the tests, the test specification and organizational issues were agreed between the participants.

All the information required to organise and manage the 1st 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 1st MCPTT Plugtests event wiki: https://wiki.plugtests.net/1st-MCPTT-Plugtest/ (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)
- MCPTT 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)

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 2017 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 2017 the vendors conducted pre-tests with each other.

ETSI has developed a test specification with 47 test cases. See clause 8. The test specification will be published as an ETSI document at ETSI TCCE (TETRA and Critical Communications Evolution).

About 1000 tests were conducted by the vendors. 85% of the tests were successful, the remaining 15% failed for various reasons. The detailed results of the tests are available for the involved vendors in this test, 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 MCPTT 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. These are given in clause 10

TCCA and ETSI plan to conduct more MCPTT Plugtests in the future. The next MCPTT Plugtests sessions are planned for Q2 2018. Vendors who have not participated in this first MCPTT Plugtest are welcome and encouraged to join the next MCPTT Plugtests event. The interest of TCCA and ETSI is to have one global standard for Mission Critical Push To Talk, which can be ensured by interoperability testing at the Plugtests.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or nonspecific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1] 3GPP TS 22.179: "Mission Critical Push to Talk (MCPTT) over LTE; Stage 1", v13.3.0.

[2] 3GPP TS 23.179: "Functional architecture and information flows to support mission critical communication services; Stage 2", v13.4.0.

[3] 3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE_LTE); Stage 2", v13.3.0

[4] 3GPP TS 24.229: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3", v13.8.0.

[5] 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control; Protocol specification", v13.3.0.

[6] 3GPP TS 24.380: "Mission Critical Push To Talk (MCPTT) media plane control; Protocol specification", v13.3.0.

[7] 3GPP TS 24.481: "Mission Critical Services (MCS) group management; Protocol specification", v13.3.0.

[8] 3GPP TS 24.482: "Mission Critical Services (MCS) identity management; Protocol specification", v13.2.0.

[9] 3GPP TS 24.483: "Mission Critical Services (MCS) Management Object (MO)", v13.3.0.

[10] 3GPP TS 24.484: "Mission Critical Services (MCS) configuration management; Protocol specification", v13.3.0.

[11] 3GPP TS 26.179: "Mission Critical Push To Talk (MCPTT); Codecs and media handling", v13.2.0.

[12] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs", v13.6.0.

[13] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points", v13.8.0,

[14] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point", v13.8.0.

[15] 3GPP TS 29.283: "Diameter Data Management Applications", v13.2.0.

[16] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE_LTE); MB2 reference point;Stage 3",v13.2.0.

[17] 3GPP TS 33.179: "Security of Mission Critical Push To Talk (MCPTT) over LTE", v13.3.0.

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

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

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

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

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

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

[24] IETF RFC 7315: "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP".

[25] 3GPP TR 23.779: "Study on application architecture to support Mission Critical Push To Talk over LTE (MCPTT) services", v13.0.0.

[26] 3GPP TR 24.980: "Minimum Requirements for support of MCPTT Service over the Gm reference point",v13.0.1.

[27] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[28] IETF RFC 3261: "SIP: Session Initiation Protocol".

[29] IETF RFC 7989: "End-to-End Session Identification in IP-Based Multimedia Communication Networks".

[30] IETF RFC 3841: "Caller Preferences for the Session Initiation Protocol (SIP)".

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].

APN	Access Point Name
AS	Application Server
BM-SC	Broadcast Multicast Service Centre
CSC	Common Services Core
eMBMS	Evolved Multimedia Broadcast and Multicast Service
eNB	Evolved Node B
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EPC	Evolved Packet Core
EPS	Evolved Packet System
ETSI	European Telecommunication Standards Institute
EUT	Equipment Under Test
FQDN	Fully Qualified Domain Name
GCS AS	Group Communication Service Application Server
GCSE_LTE	Group Communication Service Enabler over LTE
HIVE	Hub for Interoperability and Validation at ETSI
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
I-CSCF	Interrogating CSCF
ICE	Interactive Connectivity Establishment
IM CN	IP Multimedia Core Network
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public identity
IMS	IP Multimedia Subsystem
MBMS	Multimedia Broadcast and Multicast Service
MBSFN	Multimedia Broadcast multicast service Single Frequency Network
MC	Mission Critical
MCID	Mission Critical user identity
MCPTT	Mission Critical Push To Talk
MCPTT AS	MCPTT Application Server
MCPTT group ID	MCPTT group identity
MCPTT ID	MCPTT user identity
NAT	Network Address Translation
PAP	Password Authentication Protocol
P-CSCF	Proxy CSCF
PCC	Policy and Charging Control
PCRF	Policy and Charging Rules Function
ProSe	Proximity-based Services
PSI	Public Service Identity
PTT	Push To Talk
QCI	QoS Class Identifier
QoS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
S-CSCF	Serving CSCF
SDO	Standard Developing Organization
SIP	Session Initiated Protocol
TRT	TestReporting Tool
UE	User Equipment
USB	Universal Serial Bus
URI	Uniform Resource Identifier
WLAN	Wireless Local Area Network
TCCA	TETRA + Critical Communications Association

4 Technical and Project Management

4.1 Scope

The main goal of the first MCPTT Plugtests was testing the interoperability of the MCPTT ecosystem signalling and media plane at different levels.

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

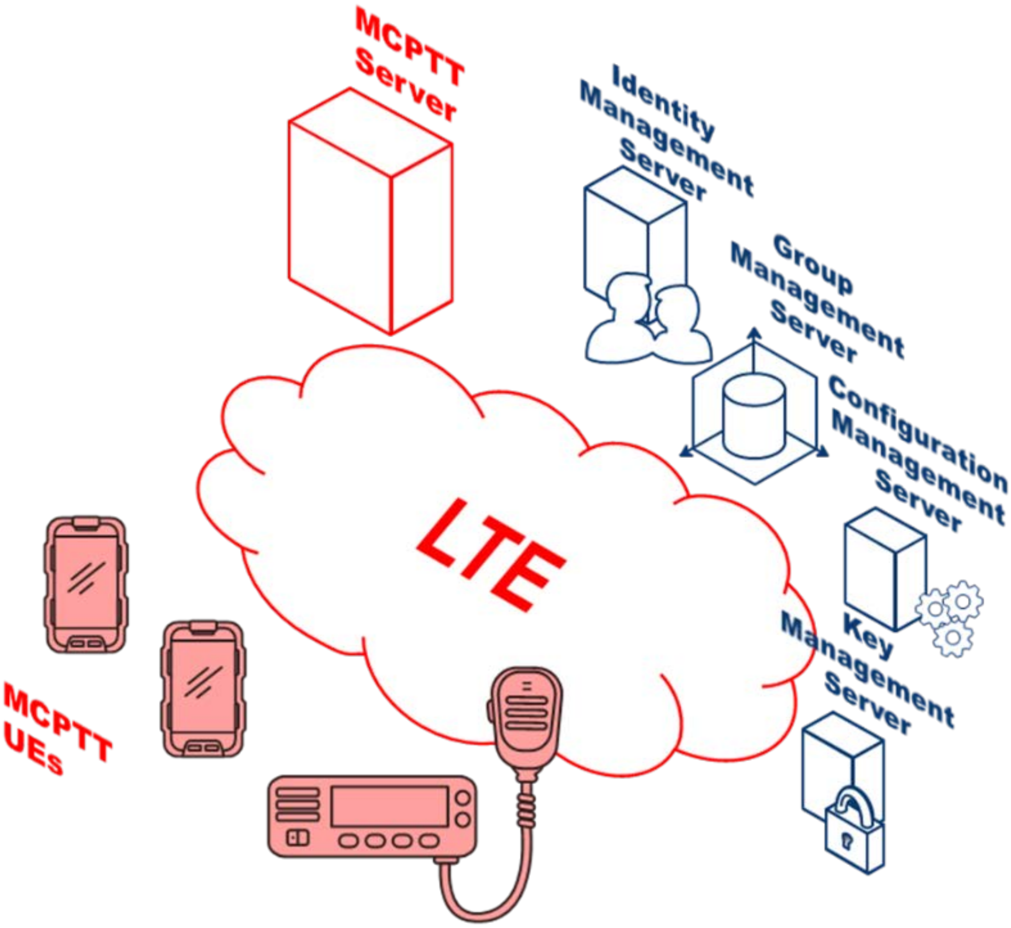

Figure 1: Typical MCPTT scenario to be considered in the plugtest

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 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 UEs to Participating/Controlling MCPTT Servers and vice versa. 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.

- **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-emptiveness mechanisms.
- **Policying (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. However, due to time constraints they were not comprehensively tested in this first.

4.2 Timeline

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

	Dec-16	Jan-17	Feb-17	Mar-17	Apr-16		May-17	Jun-17	Jul-17
Conf-Calls	7 Dec, 2PM CET	18 Jan, 2PM CET	every two weeks						
Registration	24/10/2016 - 15/01/2017								
Integration					01/04/2017 - 01/05/2017				
Pre-testing							01/5-16/6/2017		
Plugtests								19-23/6/2017	24/6-5/7/2017

Figure 2. Plugtests event timeline

Registration to the MCPTT Plugtests event was open from 24th October 2016 to 15th January 2017 to any organisation willing to participate in testing the MCPTT Ecosystem. Due to space limitations in the hosting laboratory, on-site participation was limited to 80 people at a time. Participating companies were requested to restrict on-site participation to a maximum of 2 people per equipment at a time. Additional remote participation (i.e. back office support) was possible and supported with electronic tools, see clause 4.3. A total of 140 people were involved in the Plugtests event either locally or remotely.

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, weekly conf-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 13 capabilities (December 2016 Release) 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 May 2017, 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 23 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 MCPTT servers and MCPTT Clients for 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, bi-weekly conf-calls were run among organisers and participants to synchronise, track progress and get ready for the on-site phase.

4.2.3 Plugtests event

From 19th of June to the 23rd of June, participants sent representatives to the host Lab to collaboratively run the Interoperability Test Sessions.

These 1 week on-site were organised as follows:

MCPTT#1 PLU Agenda (19 - 23 June 2017)					
Time	Monday 19	Tuesday 20	Wednesday 21	Thursday 22	Friday 23
08:30	Room Opening	Room Opening	Room Opening	Room Opening	Room Opening
09:00 13:00	SET-UP	TEST SESSION #2	TEST SESSION #4	TEST SESSION #6	TEST SESSION #8
13:00 14:00	LUNCH BREAK	LUNCH BREAK	LUNCH BREAK	LUNCH BREAK	LUNCH BREAK
14:00 18:00	TEST SESSION #1	TEST SESSION #3	TEST SESSION #5	TEST SESSION #7	TEAR-DOWN
18:00 19:00	WRAP UP	WRAP UP ends 18:45	WRAP UP	WRAP UP	
		Social event starts 19:15			

Figure 3. Plugtests event on-site HL schedule

The first half day 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 1/2 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.

4.3 Tools

4.3.1 Plugtests event Wiki

The Plugtests event Wiki was the main entry point for all the information concerning 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.
- **Network Infrastructure** - HIVE connection request tool, and remote connections status overview.
- **Equipment Under Test** - Participating EUTs overview.
- **Pre-Testing** - Remote integration and pre-testing schedule, remote integration and pre-testing procedures.
- **Plugtest Observation** - Issues found during Plugtests event with solutions.
- **Testing Information** - Access to the Test Plan, including Test Descriptions.
- **Schedule & Reporting** - Daily schedule for the on-site phase, access and documentation of the Test Reporting Tool
- **Conf-Calls** - Calendar, logistics, agendas and minutes of the weekly conf-calls run during the remote integration and pre-testing phase.
- **Wrap-up Sessions** - Agenda and minutes of the daily wrap up meetings run during the on-site phase.

In addition, an embedded Wiki Chat allowed participants to communicate during the pre-testing phase and Test Sessions, and include their remote colleagues (back-office support) in the discussions.

4.3.2 Test Session Scheduler

The Test Session Scheduler allowed the Plugtests event organisers to produce a daily schedule during the on-site phase. This tool has the following objectives:

- maximise the number of test sessions
- balance the amount of test sessions among participants
- take into account supported features of the participating FUTs
- minimise the number of participants not involved in a test session anytime.

The picture below shows a partial view a daily schedule. Each yellow box corresponds to a specific Test Session including 1 MCPTT Server, 1 MCPTT Client and 1 IMS core. For each of these sessions a Test Session Report was recorded (see next clause). An average of 14 Test Sessions were run every day during the Plugtests event.

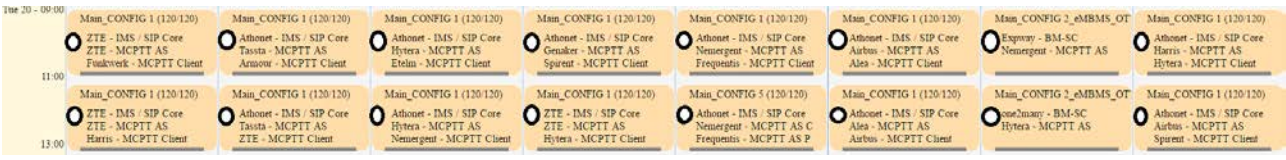

Figure 4. Daily Schedule example

4.3.3 Test Reporting Tool (TRT)

The Test Reporting Tool guides participants through the Test Plan during the on-site Test Sessions, during Pretesting and allows to create Test Session Reports compiling detailed results for the scheduled Test Sessions.

Only the companies providing the EUTs for each specific Test Session have access to the Test Session Reports contents and specific results. All the companies providing the EUTs for a Test Session, i.e. MCPTT Server, MCPTT Client and IMS core are required to verify and approve the reported results at the end of the session.

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.

2434	2017-06-20 16:00	120	Test Slot 4	Main_CONFIG 1	Athonet - IMS / SIP Core Alea - MCPTT AS Armour - MCPTT Client
2435	2017-06-20 16:00	120	Test Slot 3	Main_CONFIG 2_eMBMS_OTT	Huawei - BM-SC Hytera - MCPTT AS
2436	2017-06-20 14:00	120	Test Slot 5	Main_CONFIG 1	Athonet - IMS / SIP Core Tassta - MCPTT AS Spirent - MCPTT Client
2437	2017-06-20 14:15	120	Test Slot 6	Main_CONFIG 1	Athonet - IMS / SIP Core Airbus - MCPTT AS Armour - MCPTT Client
2438	2017-06-20 16:30	120	Test Slot 6	Main_CONFIG 1	Athonet - IMS / SIP Core Harris - MCPTT AS Airbus - MCPTT Client
2439	2017-06-20 16:15	120	Test Slot 5	Main_CONFIG 6	Athonet - ePC + eNB Nemergent - MCPTT AS Nemergent - MCPTT Client Armour - MCPTT Client
2440	2017-06-20 14:15	120	Test Slot 7	Main_CONFIG 1	Athonet - IMS / SIP Core Airbus - MCPTT AS Hytera - MCPTT Client
2441	2017-06-21 11:00	120	Test Slot 6	Main_CONFIG 1	Athonet - IMS / SIP Core Airbus - MCPTT AS Genaker - MCPTT Client
2442	2017-06-21 11:00	120	Test Slot 3	Main_CONFIG 1	Athonet - IMS / SIP Core Harris - MCPTT AS Etelm - MCPTT Client

Figure 5. Test Reporting Tool

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	No comment
Alea	Supports split operation as Participating AS and Controlling AS
Genaker	Supports split operation as Participating AS and Controlling AS
Harris Corporation	No comment
Hytera	Supports split operation as Participating AS and Controlling AS
Nemergent	Supports split operation as Participating AS and Controlling AS
TASSTA	No comment
ZTE	No comment

Table 1 MCPTT Application Servers Under Test

5.2 MCPTT Clients

Organisation	Comment
Airbus	No comment
Alea	No comment
Armour Communications	No comment
Etelm	MCPTT Client is included into the Etelm TETRA Base Station
Frequentis	MCPTT Client and MCPTT Participating AS is included into the Frequentis Control Room
Funkwerk	MCPTT Client on dedicated Cabradio-platform
Genaker	No comment
Harris Corporation	No comment
Hytera	No comment
Nemergent	No comment
Spirent	No comment
TASSTA	No comment
ZTE	No comment

Table 2 MCPTT Clients Under Test

5.3 MCPTT User Equipment

Organisation	Comment
Bittium	No comment
Funkwerk	Cab Radio

Table 3 MCPTT User Equipment Under Test

5.4 IP Multimedia Subsystem (IMS)

Organisation
Athonet

Table 4. IP Multimedia Subsystem (IMS) Under Test

5.5 LTE Network Components

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

Organisation
Athonet
Ericsson
Expway
Huawei
one2many

Table 5 LTE Network Components Under Test

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 6:

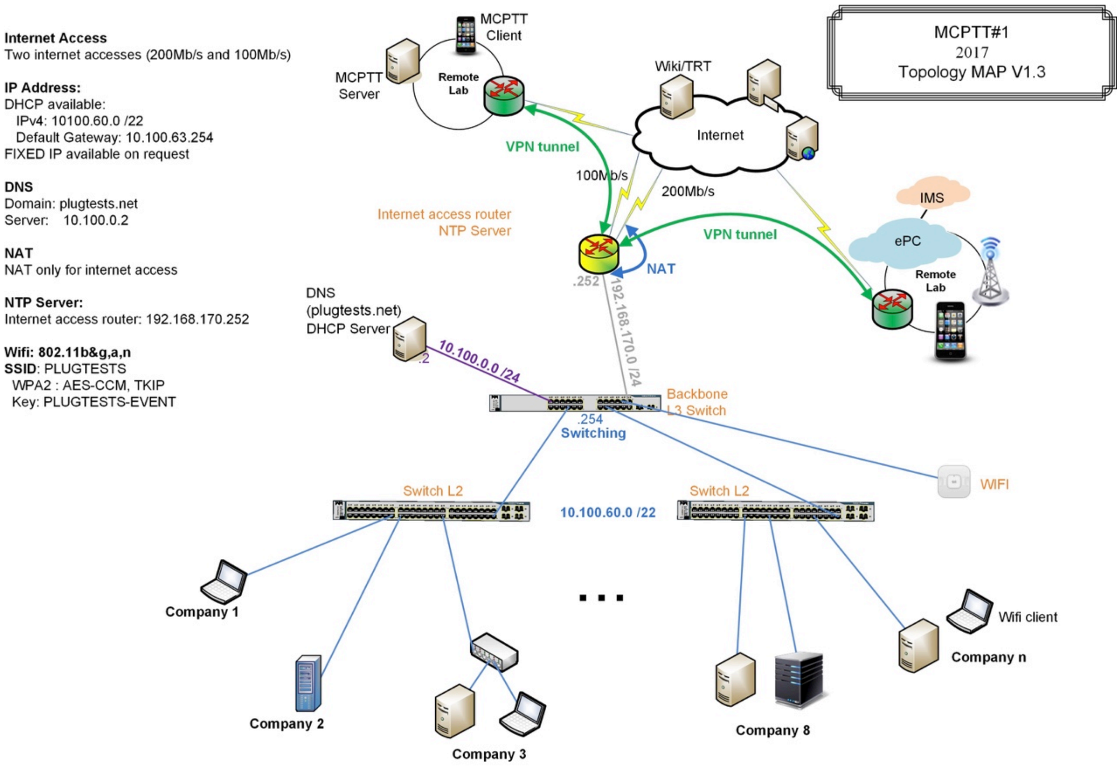

Figure 6. Remote Test Infrastructure

Once HIVE was deployed, a number of VPN tunnels were created to interconnect the equipment of the participants where the EUTs were running (MCPTT Server and MCPTT Client).

A total of 23 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 following pre-testing activities were run:

- 7.2.1 MCPTT User initiates an on-demand prearranged MCPTT Group Call [CONN/ONN/GROUP/PREA/ONDEM/NFC/01].
- 7.2.9 MCPTT User initiates an on-demand Chat Group Call [CONN/GROUP/CHAT/ONDEM/NFC/01].
- 7.2.15 MCPTT User initiates an on-demand private MCPTT call in automatic commencement model with floor control [CONN/PRIV/AUTO/ONDEM/WFC/NFC/01].
- 7.2.17 MCPTT User initiates a pre-established private MCPTT call in automatic commencement model with floor control [CONN/PRIV/AUTO/PRE/WFC/NFC/01].
- 7.4.2 MCPTT User gets registered using third-party registration [REGAUTH/3PRTY- REG/REGISTER/01].
- 7.6.1 MBMS Bearer activation upon a Group Call [EMBMS/ACTIVATEBEARER/01].
- 7.7.3 MCPTT User requests its affiliation to a set of groups [AFFIL/CHANGE/01.

The progress of these procedures for the different combinations of EUTs (MCPTT Server, MCPTT Client, IMS Core) was captured in the reporting function of TRT. The following Pre-Testing configurations were used in the pretesting phase

Pre-testing Configuration	
PreTest_CONFIG 1	MCPTT Client + MCPTT AS (Participating + Controlling) + IMS / SIP Core
PreTest_CONFIG 2	MCPTT Client + MCPTT AS (Participating + Controlling) + IMS / SIP Core + BM-SC
PreTest_CONFIG 3	MCPTT Client + MCPTT AS Participating + MCPTT AS Controlling + IMS / SIP Core
PreTest_CONFIG IMS	MCPTT Client + IMS / SIP Core

Table 6 Pre-testing Configuration

7.2 Interoperability Testing Procedure

During the on-site part of the Plugtests event, a daily Test Session Schedule was produced after discussion with all the participants. 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.

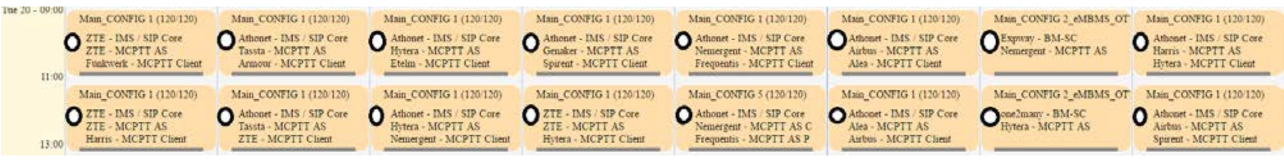

Figure 7. Daily Schedule & Test Sessions

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 + BM-SC
Main_CONFIG 2_eMBMS_OTT	BM-SC + MCPTT AS (Participating+Controlling)
Main_CONFIG 3	MCPTT Client + MCPTT AS Participating + MCPTT AS Controlling + IMS / SIP Core
Main_CONFIG 4	eNB / ePC + 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	eNB + ePC + MCPTT AS (Participating+Controlling) + IMS / SIP Core

Table 7. Main Test Configuration

The day started with a 3 hours of Warm-Up Session during which representatives of the different EUTs (MCPTT Server, MCPTT Client) that were scheduled together for the day went through a number of sanity checks in order to make sure the Test Sessions could be run smoothly. These checks included:

1. Verifying that the IMS Registration and configuration of MCPTT AS on top of IMS was working.
2. Verifying the connectivity between IMS Core.

After the Warm-up session afternoon session was scheduled for every participating EUTs.

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.

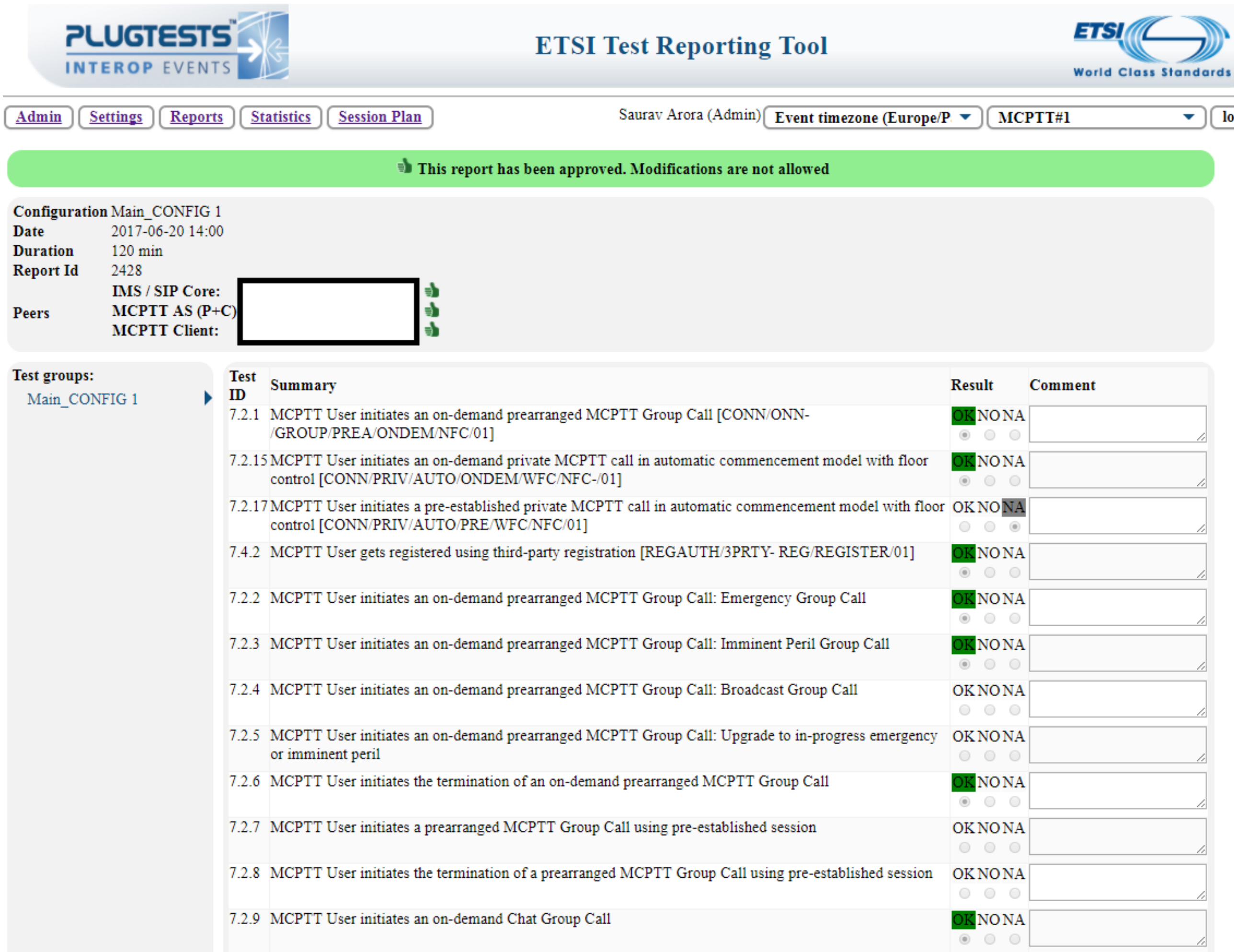

Figure 8. Test Session Report

2. For each Test in the Test Plan:

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

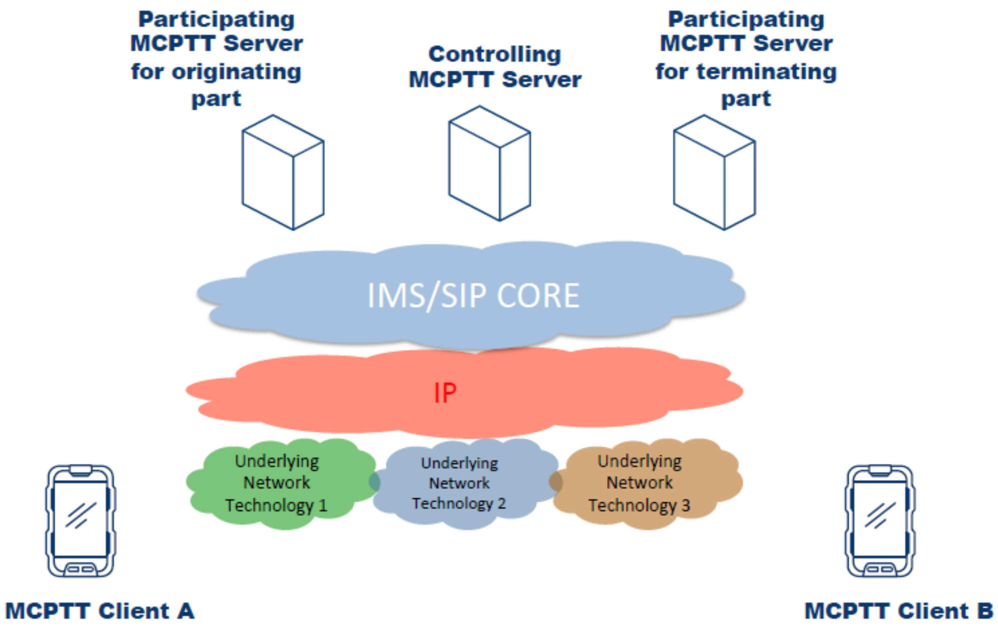

Figure 9. System Under Test (SUT) Configuration

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 10 Test Description example

3. MCPTT 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 MCPTT 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 1st MCPTT Plugtest Test Plan was developed following ETSI guidelines for interoperability. It was designed to support a series of MCPTT Plugtests events.

The Test Plan was reviewed and discussed with participants during the preparation and pre-testing phase. Furthermore, due to the extension and complexity of the test cases defined, a subset of those was selected upon consensus from participants to be a) tested in the pre-testing phase b) prioritized in the scheduling during the Plugtests event itself.

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 MCPTT ecosystem comprises both controlling and participating MCPTT application server(s), MCPTT UEs deployed over a generic SIP Core/IMS, LTE access network with and without MCPTT required PCC capabilities and native multicast support (i.e. Rel 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. Additionally, two call modes were considered in the 3GPP Rel 13 standards, On- and Off- network, according to the availability (or not) of core infrastructure. On-Network operations only were considered.

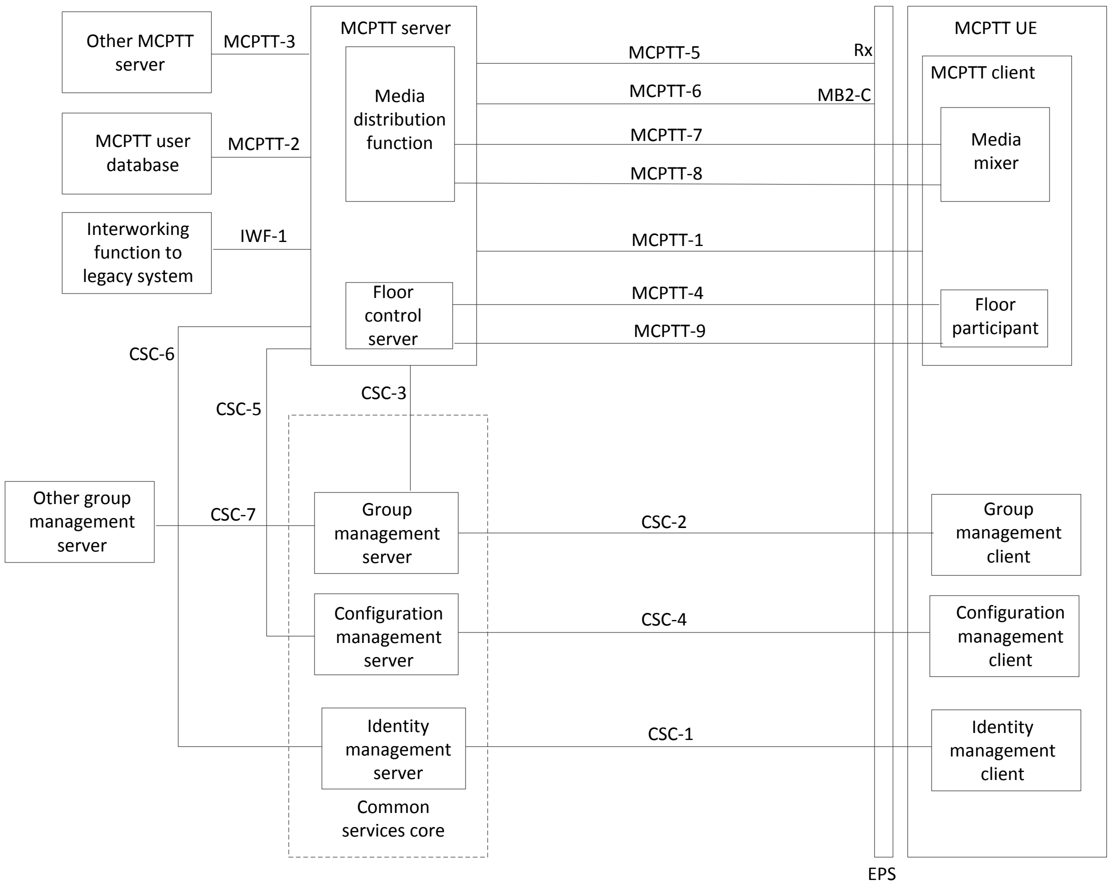

Figure 11. Functional model for application plane Figure 7.3.1-1 in 3GPP TS 23.179 [2].

Figure 7.3.1-1 in 3GPP TS 23.179 [2] describes the overall architecture and the reference points considered for the interoperability testing. As can be seen, the resulting number of functional elements, interfaces and protocols involved is quite large. Furthermore, there are MCPTT-only specific interfaces and others (like Rx and MB2-C/MB2-U) involving other supporting technologies like LTE EPS. In order to focus on MCPPT signalling the following three different configuration were initially considered: MCPTT 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 emulateds 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.

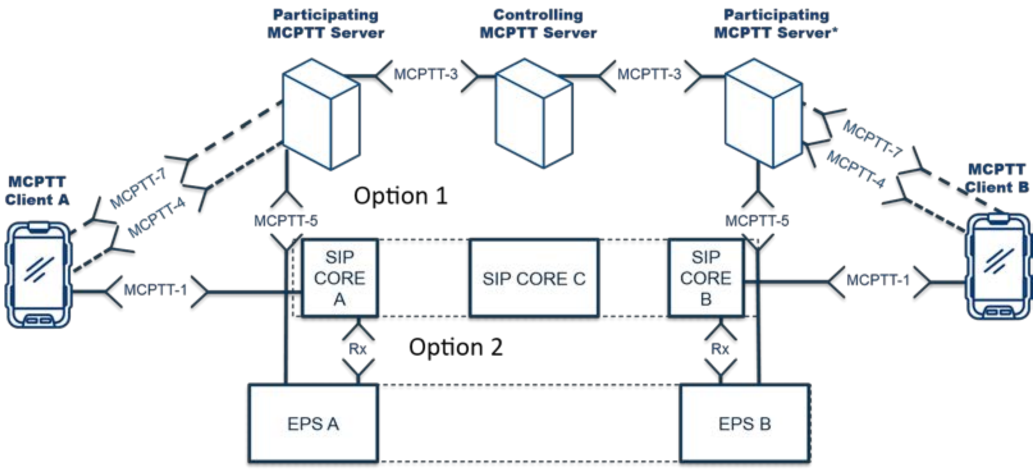

Figure 12. CFG_ONN_UNI-MC-LTE-1 configuration

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 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.

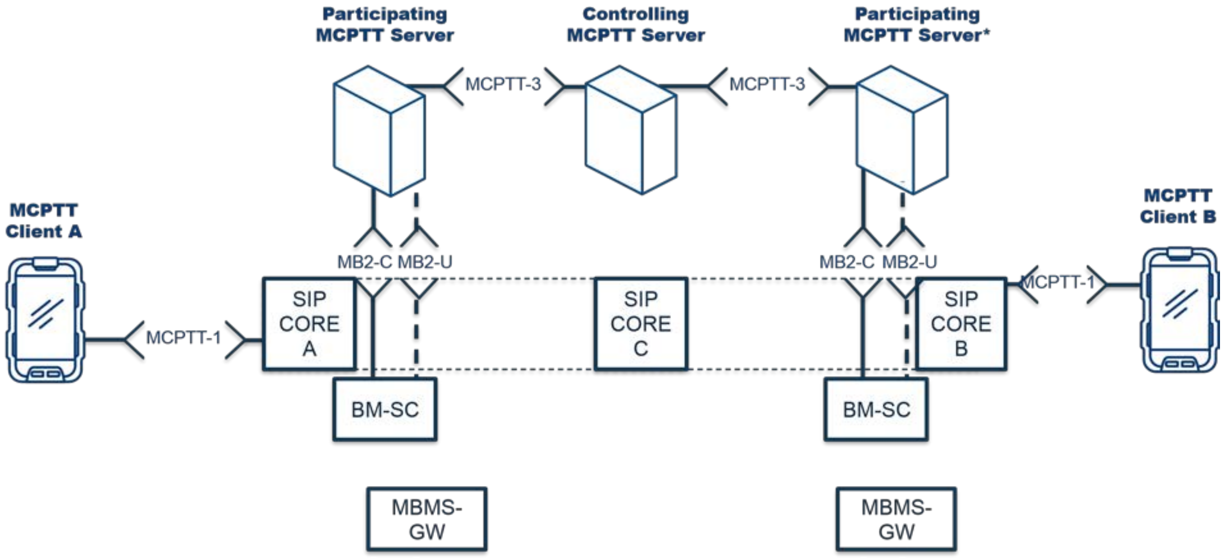

Figure 13. CFG_ONN_MULTI-MC-LTE-1 configuration

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 13 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 2_eMBMS_OTT
	Main_CONFIG 3
	Main_CONFIG 5
	Main_CONFIG 6
UNI-MC-LTE	Main_CONFIG 4
	Main_CONFIG 7
MULTI-MC-LTE	Main_CONFIG 2_eMBMS

Table 8. 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/GROUP/PREA/ONDEM/NFC/01	On-demand prearranged Group Call (Subclauses 10.1.1.2.1, 10.1.1.3.1.1 and 10.1.1.4 in 3GPP TS 24.379 [5])
CONN/GROUP/PREA/ONDEM/NFC/02	On-demand prearranged Group Call (Subclauses 10.1.1.2.1, 10.1.1.3.1.1 and 10.1.1.4 in 3GPP TS 24.379 [5]): Emergengy Group Call (6.2.8.1.[1-8][13-17] in 3GPP TS 24.379 [5])
CONN/GROUP/PREA/ONDEM/NFC/03	On-demand prearranged Group Call (Subclauses 10.1.1.2.1, 10.1.1.3.1.1 and 10.1.1.4 in 3GPP TS 24.379 [5]): Inminent Peril Group Call (6.2.8.1.9-12 in 3GPP TS 24.379 [5])
CONN/GROUP/PREA/ONDEM/NFC/04	On-demand prearranged Group Call (Subclauses 10.1.1.2.1, 10.1.1.3.1.1 and 10.1.1.4 in 3GPP TS 24.379 [5]): Broadcast Group Call (6.2.8.2 in 3GPP TS 24.379 [5])
CONN/GROUP/PREA/ONDEM/NFC/05	On-demand prearranged Group Call (Subclauses 10.1.1.2.1, 10.1.1.3.1.1 and 10.1.1.4 in 3GPP TS 24.379 [5]: Upgrade to in-progress emergency or imminent peril (10.1.1.2.1.3, 10.1.2.2.1.4 in 3GPP TS 24.379 [5])
CONN/GROUP/PREA/ONDEM/NFC/06	Termination of an on-demand prearranged Group Call (Subclauses 10.1.1.2.3.1 and 10.1.1.3.3.1 in 3GPP TS 24.379 [5])
CONN/GROUP/PREA/PRE/NFC/01	Prearranged Group Call using pre-established session (Subclauses 10.1.1.2.2, 10.1.1.3.1.2 and 10.1.1.4 in 3GPP TS 24.379 [5]
CONN/GROUP/PREA/PRE/NFC/02	Termination of a prearranged Group Call using pre-established session (Subclauses 10.1.1.2.3.2 and 10.1.1.3.3.2 in 3GPP TS 24.379 [5])
CONN/GROUP/CHAT/ONDEM/NFC/01	On-demand Chat Group Call establishment (Subclauses 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 3GPP TS 24.379 [5])
CONN/GROUP/CHAT/ONDEM/NFC/02	Ongoing on-demand Chat Group Call upgraded to emergency call (Subclauses 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 3GPP TS 24.379 [5])
CONN/GROUP/CHAT/ONDEM/NFC/03	Ongoing on-demand Chat Group Call upgraded to imminent peril (Subclauses 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 3GPP TS 24.379 [5])
CONN/GROUP/CHAT/ONDEM/NFC/04	Cancellation of the in-progress emergency condition of an on-demand Chat Group Call (Subclauses 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 3GPP TS 24.379 [5])
CONN/GROUP/CHAT/ONDEM/NFC/05	Cancellation of the in-progress imminent peril condition of an on-demand Chat Group Call (Subclauses 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 3GPP TS 24.379 [5])
CONN/GROUP/CHAT/PRE/NFC/01	Chat Group Call establishment within a pre-established session (Subclauses 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 3GPP TS 24.379 [5])
CONN/PRIV/AUTO/ONDEM/WFC/NFC/01	On-demand private call with floor control (Subclause 11.1.1.2.1 in 3GPP TS 24.379 [5]) and automatic commencement mode (see IETF RFC 5373 [21])
CONN/PRIV/MAN/ONDEM/WFC/NFC/01	On-demand private call with floor control manual mode (Subclause 11.1.1.2.1 in 3GPP TS 24.379 [5]) and manual commencement mode (see IETF RFC 5373 [21])
CONN/PRIV/AUTO/PRE/WFC/NFC/01	Pre-established private call with floor control (Subclause 11.1.1.2.1 in 3GPP TS 24.379 [5]) and automatic commencement mode (see IETF RFC 5373 [21])
CONN/PRIV/MAN/PRE/WFC/NFC/01	Pre-established private call with floor control manual mode (Subclause 11.1.1.2.1 in 3GPP TS 24.379 [5]) and manual commencement mode (see IETF RFC 5373 [21])
CONN/PRIV/AUTO/ONDEM/WOFC/01	On-demand private call without floor control (Subclause 11.1.1.2.1 in 3GPP TS 24.379 [5]) and automatic commencement mode (see IETF RFC 5373 [21])
CONN/PRIV/MAN/ONDEM/WOFC/01	On-demand private call without floor control manual mode (Subclause 11.1.1.2.1 in 3GPP TS 24.379 [5]) and manual commencement mode (see IETF RFC 5373 [21])
CONN/PRIV/AUTO/PRE/WOFC/01	Pre-established private call without floor control (Subclause 11.1.1.2.1 in 3GPP TS 24.379 [5]) and automatic commencement mode (see IETF RFC 5373 [21])

Table 9. Test Group for the Connectivity (CONN) objective

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

Table 10. Test Group for the Floor Controlling (FC) objective

Test Id	Test Purpose
REGAUTH/IDMSAUTH/01	MCPTT Client authentication and tokens retrieval using IdMS 3GPP TS 24.482 [8]
REGAUTH/3PRTYREG/REGISTER/01	MCPTT Client registration using 3rd party register (Subclauses 7.2.1 and 7.3.2 in 3GPP TS 24.379 [5])
REGAUTH/PUBLISH/REGISTER/01	MCPTT Client registration using SIP PUBLISH (Subclauses 7.2.2 and 7.3.3 in 3GPP TS 24.379 [5])

Table 11. Test Group for the Registration and Authorization (REGAUTH) objective

Test Id	Test Purpose
PCC/BEARERSETUP/01	Unicast MC Bearer Setup by SIP Core/IMS (Subclauses 4.4.1 and 4.4.2 in 3GPP TS 29.214 [14])
PCC/BEARERSETUP/02	Unicast MC Bearer Setup by MCPTT Participating AS (Subclauses 4.4.1 and 4.4.2 in 3GPP TS 29.214 [14])
PCC/BEARERUPDATE/01	Unicast MC Bearer Update by SIP Core/IMS due to a change in the Call characteristics (i.e. upgrade to emergency call)
PCC/BEARERUPDATE/02	Unicast MC Bearer Update by MCPTT Participating AS due to a change in the Call characteristics (i.e. upgrade to emergency call)

Table 12. Test Group for the Policying (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 [16])
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 13. 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 [5])
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 [5])
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 [5])
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 [5])
AFFIL/CHANGE/03	Affiliation status change triggered by another MCPTT User in negotiated mode (Subclauses 9.2.1.4 and 9.2.1.5 in 3GPP TS 24.379 [5])

Table 14. 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 [5])
LOC/REQUEST/01	Request for Location Report to the MCPTT Client (Subclauses 13.2.3 and 13.3.3 in 3GPP TS 24.379 [5])
LOC/SUBMISSION/01	MCPTT Client Sends location upon trigger (Section 13.3.4 in 3GPP TS 24.379 [5])

Table 15. Test Group for the Location (LOC) objective

9 Interoperability Results

9.1 Overall Results

During the Plugtests event, a total of 160 Test Sessions were run: that is, 160 different combinations based on different configurations in Test Scope: MCPTT Client, MCPTT Server (Participating and Controlling), UE, eNB and IMS/SIP Core were tested for interoperability. Overall, over 900 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		Execution Rate	
OK	NO	NA	Run
811 (85.5%)	138 (14.5%)	2112 (69.0%)	949 (31.0%)

Table 16: Overall Results

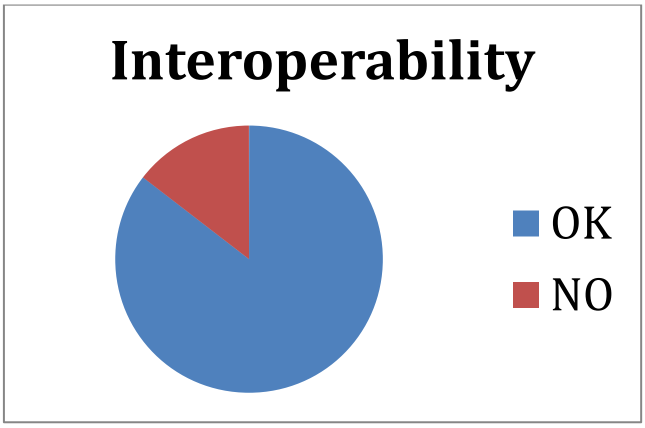

Figure 14. Overall results (%)

The overall interoperability rate of 85.5 % 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.

	Interoperability		Execution Rate	
	OK	NO	NA	Run
PreTest_CONFIG 1	89 (70.6%)	37 (29.4%)	79 (38.5%)	126 (61.5%)
PreTest_CONFIG 2	2 (100.0%)	0 (0.0%)	0 (0.0%)	2 (100.0%)
PreTest_CONFIG IMS	11 (100.0%)	0 (0.0%)	0 (0.0%)	11 (100.0%)
PreTest_CONFIG 3	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
Main_CONFIG 1	634 (87.6%)	90 (12.4%)	1701 (70.1%)	724 (29.9%)
Main_CONFIG 2_eMBMS	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
Main_CONFIG 3	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
Main_CONFIG 4	25 (75.8%)	8 (24.2%)	116 (77.9%)	33 (22.1%)
Main_CONFIG 2_eMBMS_OTT	14 (87.5%)	2 (12.5%)	16 (50.0%)	16 (50.0%)
Main_CONFIG 5	31 (96.9%)	1 (3.1%)	166 (83.8%)	32 (16.2%)
Main_CONFIG 6	5 (100.0%)	0 (0.0%)	34 (87.2%)	5 (12.8%)

Table 17. 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 Case #	Interoperability	
	OK	NO
7.2.1	70 (71.4%)	28 (28.6%)
7.2.15	75 (80.6%)	18 (19.4%)
7.2.17	3 (23.1%)	10 (76.9%)
7.4.2	122 (99.2%)	1 (0.8%)
7.6.1	2 (100.0%)	0 (0.0%)
TC IMS	11 (100.0%)	0 (0.0%)
7.2.2	25 (89.3%)	3 (10.7%)
7.2.3	21 (87.5%)	3 (12.5%)
7.2.4	20 (90.9%)	2 (9.1%)
7.2.5	7 (58.3%)	5 (41.7%)
7.2.6	49 (84.5%)	9 (15.5%)
7.2.7	0 (0.0%)	3 (100.0%)
7.2.8	0 (0.0%)	1 (100.0%)
7.2.9	36 (97.3%)	1 (2.7%)
7.2.11	6	0

	(100.0%)	(0.0%)
7.2.10	7 (87.5%)	1 (12.5%)
7.2.12	6 (100.0%)	0 (0.0%)
7.2.13	6 (100.0%)	0 (0.0%)
7.2.14	0 (0.0%)	1 (100.0%)
7.2.16	51 (94.4%)	3 (5.6%)
7.2.18	1 (100.0%)	0 (0.0%)
7.2.19	21 (91.3%)	2 (8.7%)
7.2.20	25 (92.6%)	2 (7.4%)
7.3.1	54 (80.6%)	13 (19.4%)
7.3.2	34 (75.6%)	11 (24.4%)
7.4.1	3 (60.0%)	2 (40.0%)
7.5.2	2 (100.0%)	0 (0.0%)
7.6.2	2 (100.0%)	0 (0.0%)
7.6.3	4 (100.0%)	0 (0.0%)
7.6.5	1 (100.0%)	0 (0.0%)
7.6.6	1	0

	(100.0%)	(0.0%)
7.6.7	2 (100.0%)	0 (0.0%)
7.6.8	3 (75.0%)	1 (25.0%)
7.6.9	1 (50.0%)	1 (50.0%)
7.7.1	64 (97.0%)	2 (3.0%)
7.7.2	6 (75.0%)	2 (25.0%)
7.7.3	55 (87.3%)	8 (12.7%)
7.7.4	3 (75.0%)	1 (25.0%)
7.7.5	0 (0.0%)	1 (100.0%)
7.8.1	4 (80.0%)	1 (20.0%)
7.8.2	1 (50.0%)	1 (50.0%)
7.4.3	7 (87.5%)	1 (12.5%)

Table 18

10 Base Specification Validation

As a result of the Plugtests event activities some issues in 3GPP Technical Specifications (TSs) and related standards were identified together with deployment practical 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 MCPTT vendors in most deployments.

The reader should note that 3GPP TS approved in December 2016 (mostly 13.3.0) were considered for the first Plugtests event and some fields may have changed or have been already solved.

1st MCPTT Plugtests event team wants to thank all the participants in the Plugtest 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 MCPTT Standards issues

10.1.1 Typo in mpctt-info root element

In the mcptt-info schema associated to 3GPP TS.24.379 v13.30, mcptt info is wrongly depicted as mpcttinfo.

```
<!-- root XML element -->

<xs:element name="mpcttinfo" type="mcpttinfo:mcpttinfo-Type" id="info"/>

…
```

10.1.2 Missing Client ID in 3rd party REGISTER based service authorization

According to 3GPP TS 24.379 [5] MCPTT user registration and authorization procedure can use 3rd party REGISTER only or demand a later PUBLISH message depending on the IdMS registration sequence. In subclause 7.2.2 of 3GPP TS 24.379 [5], the client ID

(<mcptt-client-id> element) is included in the PUBLISH body but it is not included in subclause 7.2.1 for the REGISTER message. In order to use 3rd party registration only the client ID should be also included.

10.1.3 Missing reference to Location configuration message upon PUBLISH based authorization

Similarly to the previous case, the location configuration mechanism in subclause 13.2.2 3GPP TS 24.379 [5] denotes that "Upon receipt of a third-party SIP REGISTER request for an MCPTT client, the participating MCPTT function may configure the location reporting in the MCPTT client by generating a SIP MESSAGE. However, if no credentials are cached and no id/access-token are initially retrieved from the IdMS the mcptt-id of the user will not be available, and therefore step 3) in 13.2.2 "shall include an application/vnd.3gpp.mcptt-info+xml MIME body with an <mcptt-request-uri> element containing the MCPTT ID of the MCPTT user to receive the configuration" would not be applicable. A reference to "subsequent PUBLISH"-triggered location configuration mechanism should be included.

10.1.4 Granted SSRC coding

The Floor Granted and Floor Taken messages in 3GPP TS 24.380 [6] include the SSRC of the granted floor participant. This is an additional field beyond the normal SSRC field in the second 32-bit word of the RTCP message

(i.e. the Floor Granted message)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|V=2|P| Subtype |   PT=APP=204  |          length               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                SSRC of floor control server                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         name=MCPT                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Duration field                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                SSRC of granted floor participant field        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Floor Priority field                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       User ID field                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Queue Size field                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              SSRC of queued floor participant field           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Queued User ID field                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Queue Info field                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Track Info field                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Floor Indicator field                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Under this diagram, the TS states that “With the exception of the three first 32-bit words the order of the fields are irrelevant.” However, since SSRC fields have no type and length in front of them un-ambiguous parsing is not possible. So, either the order of the fields should be defined or a type and length should be added to SSRC field. Furthermore, for the latter padding bytes should be agreed in order

During the plugtest the following convention was proposed

(and used):

A new SSRC field with the same format as Granted Party’s Identity field.

A new SSRC field id code 014 added to Table 8.2.3.1-2. Length set to 4 bytes

(32 bits) and coding according to the following

TLV + SSRC aligned to 4 bytes with 2 padding initial bytes

| SSRC field ID = 014 | SSRC field length = 6 | spare | spare |

| SSRC |

Additionally subclauses 8.2.3.6, 8.2.3.8 and 8.2.3.11 state that “If the length of the <XXX> value is not a multiple of 4 bytes, the XXX field shall be padded to a multiple of 4 bytes. The value of the padding bytes is set to zero. The padding bytes are ignored by the receiver.” Being XXX

However, in order to align the value to a multiple of 4 bytes the length should be a

(multiple of 4) + 2 because the length does not include the field ID and field length bytes.

10.2 Technical Constraints

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.

Additionally, other common needs for clarification have been gathered

(collected as CLARIFICATION) from some participants. Examples in each affected TS Annex(es) or associated TR were proposed as possible solutions.

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 ins 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: Selective (de)affiliation to a specific subset of groups

In the affiliation procedures in subclause 9 in 3GPP TS 24.379 [5] it was not clear for some participants whether a PUBLISH actually meant an incremental update of the subscription to the included list of group or current actual overall subscription status (thus, self contained).

According to the following table in IETF RFC 3903 [20], in order to remove all groups from the server a PUBLISH request without a body and Expires header = 0 should be sent. If the client wants to perform any modification in the current status of the group affiliations a PUBLISH request with Expires > 0 value should be sent to the server

(4294967295 in MCPTT case).

Operation	Body?	SIP-If-Match?	Expires Value
Initial	yes	no	> 0
Refresh	no	yes	> 0
Modify	yes	yes	> 0
Remove	no	yes	0

After some discussions the participants came to the common understanding that, if a MCPTT user wants to modify the current status of the affiliated groups, it will send a PUBLISH request with ALL the groups he is interested in and those not included must to be considered as NO longer interesting for the user.

(therefore de-affiliating the user). The Expires header value of this request will be 4294967295. If the client is no longer interested in any group, he will send a PUBLISH request without a body. This request will include an Expires header set to 0. It was not clear however what was the procedure to be carried out for refreshes. According to the table above, a PUBLISH request will be sent without a body. This will include an Expires header set to 4294967295.

10.2.5 CLARIFICATION: Broadcast calls release mechanism

Different implementations of broadcast group call considered an alternative behaviour for call termination. According to stage 1 3GPP TS 22.179 [1] subclause 10.6.2.5 when the media transmission from call originating MCPTT user is complete, the broadcast Group Call should be released. However no specific reference to the broadcast call termination procedure in 3GPP TS 24.379 [5] for the On-Network case was identified.

10.2.6 CLARIFICATION: Configuration of MCPTT APN

3GPP TR 24.980 [26] v13.1.0

(2016-06) “Minimum Requirements for support of MCPTT Service over the Gm reference point” defines the “MCPTT related APN” as “an APN utilised by the MCPTT service including the MCPTT service APN for the SIP-1 reference point, an MC common core services APN for the HTTP-1 reference point and a MC identity management service APN for the CSC-1 reference point.”. Furthermore, subclauses 5.2.9.2.[1-3] in 3GPP TS 23.179 [2] state that “The QCI value of 69

(as specified in 3GPP TS 23.203 [4]) shall be used for the EPS bearer that transports SIP-1 reference point messaging”, “the QCI value 8

(as specified in 3GPP TS 23.203 [4]) or better shall be used for the EPS bearer that transports HTTP-1 reference point messaging” and “The dedicated bearer for voice and MCPTT-4 reference point messaging shall utilise the QCI value of 65

(as specified in 3GPP TS 23.203 [4])."

However there is no common agreement on the characteristics of such dedicated MCPTT APN

(if any): for example, whether an QCI 65 Dedicated Bearer should be automatically setup for the SIP-1 reference point or use from the beginning that QCI for the Default Bearer

(considering SIP-1 traffic only). Considering that most probably the UE would have a general purpose APN for Data, an additional one for VoLTE and the MCPTT “dedicated one” the participants involved in the UNI-MC-LTE configuration test cased agreed that a reasonable approach would be the latter

(following somehow a behaviour similar to IR.92 profile for VoLTE): defining a MCPTT APN a default bearer with QCI 69 and dynamically establishing via PCC

(Rx/MCPTT-5) the Dedicated Bearer with QCI 65 for the media plane

(audio + floor control). Such dynamic behaviour was the one tested during the plugtest.

10.2.7 CLARIFICATION: Encoding of <entry> “uri” attribute in REFER in pre-established sessions

The usage and description of the encoding of the body in the <entry> “uri” attribute as an HTTP request

(eg. subclause 10.1.2.2.2.1 in 3GPP TS 24.379 [5]) in the resource-lists XML of the REFER for pre-established calls were considered too complex. To some partners it resulted difficult to format and more difficult to parse. There was some comment towards a possible alternative use of HTTP request as a MIME body in the multipart body of the SIP REFER message instead.

10.2.8 CLARIFICATION: Inclusion of Answer-Mode header in group calls

subclause 10.1.1.2.1.2, step 8 in 3GPP TS 24.379 [5] states that the client should check the Answer-Mode header field to determine if auto or manual commencement mode should be employed. The e2e signalling mechanism is clearly specified for private calls but apparently not that clearly for group calls. More specifically, in the originating participating function the need for stripping the header out is mentioned. Later, for the handling of the Answer-Mode header in the terminating participating function it states that “if the SIP INVITE request…. does not contain an Answer-Mode header field …” but who (the originating participating or the controlling) and under which conditions should include that header is not clearly stated.

10.2.9 CLARIFICATION: Specific reference to out-of-dialog REFER in the group calls using pre-established session

Subclause 11.1.1.2.2.1 in 3GPP TS 24.379 [5] explicitly defines the out-of-dialog nature of the SIP REFER messages: "shall generate an initial SIP REFER request outside a dialog in accordance with the procedures specified in 3GPP TS 24.229 [4], IETF RFC 4488 [22] and IETF RFC 3515 [25] as updated by IETF RFC 6665 [26] and IETF RFC 7647 [27];" while subclauses 10.1.1.2.2.1 and 10.1.2.2.2.1 for group calls don't specify. An equivalent statement should be used if that is the case.

10.2.10 CLARIFICATION: CMS Service Configuration Document location

How to address the Service Configuration Document is apparently not clearly stated. Therefore, would the user

(XUI) it is stored under be implementation specific? If this is the case it is not clear how do the MCPTT UEs and the MCPTT server know where to retrieve this document from

(i.e. both XUI and document name would be needed).

10.2.11 CLARIFICATION: UE (Init) configuration documents generation

In 3GPP TS 24.484 [10], the configuration mechanism seems to mean that the UE

(initial) configuration document would act as a master document while the actual documents would be generated on the fly upon a UE request. Similarly to previous case the XUI value used to request the document and the document name would be unclear. Furthermore the device management component responsible for that

(Device Management/XDMS/CMS) would be also unclear.

History

Document history		
V0.0.1	22/06/2017	First Draft
V0.0.2	03/07/2017	Adding Plugtests procedure.
V0.0.3	07/07/2017	Adding Plugtests observations.
V0.0.4	20/07/2017	Adding Plugtests Introduction and Executive summary.
V0.0.5	24/07/2017	Adding Plugtests Results.
V0.0.6	28/07/2017	Formatting and removing minor issues.
V1.0.0	28/07/2017	Test Report Final Version