3GPP TR 23.778 V16.0.0 (2019-06)

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Study on Mission Critical services access aspects

(Release 16)

** 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.  
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.  
This Report is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

<keyword[, keyword]>

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

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

Internet

http://www.3gpp.org

***Copyright Notification***

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2019, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword [5](#__RefHeading___Toc11676889)

Introduction [5](#__RefHeading___Toc11676890)

1 Scope [6](#__RefHeading___Toc11676891)

2 References [6](#__RefHeading___Toc11676892)

3 Definitions, symbols and abbreviations [7](#__RefHeading___Toc11676893)

3.1 Definitions [7](#__RefHeading___Toc11676894)

3.2 Symbols [7](#__RefHeading___Toc11676895)

3.3 Abbreviations [7](#__RefHeading___Toc11676896)

4 Key issues [7](#__RefHeading___Toc11676897)

4.1 IOPS related key issues [7](#__RefHeading___Toc11676898)

4.1.1 Key issue 2-1 MC system configuration data synchronization [7](#__RefHeading___Toc11676899)

4.1.1.1 Description [7](#__RefHeading___Toc11676900)

4.1.2 Key issue 2-2 MC service client configuration for IOPS [8](#__RefHeading___Toc11676901)

4.1.2.1 Description [8](#__RefHeading___Toc11676902)

4.1.3 Key issue 2-3 on how to handle an MC UE switching to/from an IOPS MC system [8](#__RefHeading___Toc11676903)

4.1.3.1 Description [8](#__RefHeading___Toc11676904)

4.1.4 Key issue 2-4 IOPS architecture [8](#__RefHeading___Toc11676905)

4.1.4.1 Description [8](#__RefHeading___Toc11676906)

4.1.5 Key issue 2-5 on ongoing communication continuity when backhaul is recovered [9](#__RefHeading___Toc11676907)

4.1.5.1 Description [9](#__RefHeading___Toc11676908)

4.1.6 Key issue 2-6 on support MBMS in IOPS [9](#__RefHeading___Toc11676909)

4.1.6.1 Description [9](#__RefHeading___Toc11676910)

4.1.7 Key issue 2-7 on determining a list of MC users connected to the IOPS MC system [10](#__RefHeading___Toc11676911)

4.1.7.1 Description [10](#__RefHeading___Toc11676912)

5 Architectural requirements [10](#__RefHeading___Toc11676913)

5.1 IOPS related requirements [10](#__RefHeading___Toc11676914)

6 Solutions [11](#__RefHeading___Toc11676915)

6.1 Solution 1: UE and user data synchronization [11](#__RefHeading___Toc11676916)

6.1.1 Description [11](#__RefHeading___Toc11676917)

6.1.2 Impacts on existing nodes and functionality [13](#__RefHeading___Toc11676918)

6.1.3 Solution evaluation [13](#__RefHeading___Toc11676919)

6.2 Solution 2: Functional model for IOPS based on a switchable standalone MC system [13](#__RefHeading___Toc11676920)

6.2.1 Description [13](#__RefHeading___Toc11676921)

6.2.2 Solution evaluation [14](#__RefHeading___Toc11676922)

6.3 Solution 3: Functional model for IOPS based on an always-on partner MC system [14](#__RefHeading___Toc11676923)

6.3.1 Description [14](#__RefHeading___Toc11676924)

6.3.2 Solution evaluation [15](#__RefHeading___Toc11676925)

6.4 Solution 4: Functional model for IOPS MC system based on only IP connectivity [15](#__RefHeading___Toc11676926)

6.4.1 Description [15](#__RefHeading___Toc11676927)

6.4.1.1 General [15](#__RefHeading___Toc11676928)

6.4.1.2 IOPS-based discovery procedure [17](#__RefHeading___Toc11676929)

6.4.1.3 IOPS-based IP connectivity communication [19](#__RefHeading___Toc11676930)

6.4.2 Impacts on existing nodes and functionality [23](#__RefHeading___Toc11676931)

6.4.3 Solution evaluation [23](#__RefHeading___Toc11676932)

6.5 Solution 5: Functional model for IOPS based on an always-on participating server [23](#__RefHeading___Toc11676933)

6.5.1 Description [23](#__RefHeading___Toc11676934)

6.5.2 Solution evaluation [25](#__RefHeading___Toc11676935)

6.6 Solution 6: Procedure for switching from the primary MC system to an IOPS MC system [25](#__RefHeading___Toc11676936)

6.6.1 Description [25](#__RefHeading___Toc11676937)

6.6.2 Procedure [25](#__RefHeading___Toc11676938)

6.6.3 Solution evaluation [27](#__RefHeading___Toc11676939)

6.7 Solution 7: IOPS notification to MC UEs [27](#__RefHeading___Toc11676940)

6.7.1 Description [27](#__RefHeading___Toc11676941)

6.7.2 Impacts on existing nodes and functionality [28](#__RefHeading___Toc11676942)

6.7.3 Solution evaluation [28](#__RefHeading___Toc11676943)

6.8 Solution 8: MC service client configuration for IOPS [29](#__RefHeading___Toc11676944)

6.8.1 Description [29](#__RefHeading___Toc11676945)

6.8.2 Solution evaluation [29](#__RefHeading___Toc11676946)

6.9 Solution 9: Functionality for determining the MC user registration status in IOPS [29](#__RefHeading___Toc11676947)

6.9.1 Description [29](#__RefHeading___Toc11676948)

6.9.2 Solution evaluation [32](#__RefHeading___Toc11676949)

7 Overall evaluation [33](#__RefHeading___Toc11676950)

7.1 General [33](#__RefHeading___Toc11676951)

7.2 Architecture evaluation [33](#__RefHeading___Toc11676952)

7.3 Key issue and solution evaluation [34](#__RefHeading___Toc11676953)

8 Conclusions [35](#__RefHeading___Toc11676954)

Annex A: Change history [36](#__RefHeading___Toc11676955)

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

# Introduction

Mission critical services can be provided even in the case of a backhaul failure or a nomadic EPS deployment based on the availability of Isolated E-UTRAN Operations for Public Safety (IOPS). IOPS provides local connectivity to the public safety users that are within the communication range of the radio base station(s) that supports the IOPS mode of operation, as described in 3GPP TS 23.401 Annex K [10].

This study focuses on identifying application architecture solutions needed to support mission critical services during the IOPS mode of operation.

# 1 Scope

This technical report is a study of mission critical service access aspects. The present document identifies architecture enhancements needed to support mission critical services delivered over IOPS, based on the stage 1 requirements, including 3GPP TS 22.179 [2], 3GPP TS 22.280 [3], 3GPP TS 22.281 [4], 3GPP TS 22.282 [5] and 3GPP TS 22.346 [6].

This document provides recommendations for normative work.

# 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 non‑specific.

- 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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.179: "Mission Critical Push to Talk (MCPTT); Stage 1".

[3] 3GPP TS 22.280: "Mission Critical Services Common Requirements".

[4] 3GPP TS 22.281: "Mission Critical Video services".

[5] 3GPP TS 22.282: "Mission Critical Data services".

[6] 3GPP TS 22.346: "Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety; Stage 1".

[7] 3GPP TS 23.280 "Common functional architecture to support mission critical services; Stage 2"

[8] 3GPP TS 23.282 "Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2"

[9] 3GPP TS 23.379: "Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2"

[10] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access"

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**IOPS MC system:** The collection of applications, services and enabling capabilities that provides MC services in an IOPS network.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.401 [10] apply:

**Local EPC**

**IOPS network**

**Macro EPC**

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] 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 [1].

IOPS Isolated E-UTRAN Operations for Public Safety

# 4 Key issues

## 4.1 IOPS related key issues

### 4.1.1 Key issue 2-1 MC system configuration data synchronization

#### 4.1.1.1 Description

An MC service operating in an IOPS mode is completely or partly isolated from the network and application infrastructure normally utilized. This requires that MC system configuration data in the IOPS MC system needs to be up to date with MC system configuration data in the primary MC system. The invocation of the MC service in IOPS mode is in most scenarios unpredictable, which also stipulate strong requirements on data synchronization between the IOPS MC system and the primary MC system.

To define an efficient MC system configuration data synchronization process, the following areas should be further studied:

- What parts of the MC system configuration data needs to be synchronized between the IOPS MC system and primary MC systems before, during and after operating in IOPS mode.

- Triggers of data synchronizations

- Service limitations due to data synchronization issues

### 4.1.2 Key issue 2-2 MC service client configuration for IOPS

#### 4.1.2.1 Description

IOPS MC system is completely or partly isolated from the network and application infrastructure normally utilized. For the MC service client to access the IOPS MC system, the client shall be configured with access information (e.g. server addresses) of the IOPS MC system. This introduce challenges when configuring MC service clients with access information to all IOPS capable eNBs in a network.

To define procedures for MC service client and UE configuration of IOPS MC system access data, the following areas should be further studied:

- What MC service client and UE data are required to be configured for accessing a IOPS MC system.

- How should this configuration be done.

- How to handle migrating users from partner system.

- Any differences from a procedural perspective in IOPS mode due to backhaul failure or limited backhaul or in IOPS mode in nomadic deployments.

### 4.1.3 Key issue 2-3 on how to handle an MC UE switching to/from an IOPS MC system

#### 4.1.3.1 Description

IOPS MC system is completely or partly isolated from the network and application infrastructure normally utilized. When MC users are located within the coverage or in proximity of an eNB in IOPS mode, the MC users may experience an unpredictable user experience, if MC UEs are switching between the IOPS enabled eNB and an eNB that is connected to the primary MC system.

This issue may be common when the IOPS enabled eNB is a macro site, and there are several smaller cells in the area of the coverage of the macro site. It is important to have a mechanism in place to get an optimize user experience when MC UEs are switching to and from the IOPS MC system.

Further study is needed to:

- Optimize the benefit for mission critical functionality to MC UEs in overlapping primary MC system and IOPS MC system operational areas.

### 4.1.4 Key issue 2-4 IOPS architecture

#### 4.1.4.1 Description

The IOPS MC system can be used through a local EPS both during backhaul failure as well as in nomadic deployment (e.g. in cell on wheel configuration). However, the IOPS MC system may be accessed by an MC UE both during IOPS operation mode and during non IOPS mode (i.e. this system may be operational already before entering IOPS mode) and in that scenario through the primary EPS or other access network. To support this, different architectural requirements and solutions should be evaluated.

Further study is needed to:

- Evaluate different architecture alternatives for an IOPS MC system

- Define the functional model used in the IOPS MC system.

- Conclude on architectural requirements for the IOPS MC system.

### 4.1.5 Key issue 2-5 on ongoing communication continuity when backhaul is recovered

#### 4.1.5.1 Description

When the backhaul of an eNB to Macro EPC is broken, the eNB enters IOPS mode and connects to the Local EPC, and the MC users served by this eNB will connect to the IOPS MC system.

After some time, the backhaul is recovered, then this eNB switches back to normal mode and re-connects to the Macro EPC, and the users served by this eNB will re-connect to the Primary MC system. This scenario is illustrated in Figure 1. At the transition time, there is a call ongoing in the IOPS MC system. Re-connecting to the Primary MC system will likely cause the termination of the ongoing communication in the IOPS MC system. However, it is beneficial to minimize the disruption to ongoing communication during the transition.



Figure 4.2.5.1-1: Ongoing communication continuity when backhaul is recovered

Further study is needed:

- Understand how communications are re-established in the Primary MC system including how group members join group communications in progress in the Primary MC system;

- How to handle call collisions if calls are ongoing in the same group in both the Primary MC system and IOPS MC system;

- How the ongoing communication continuity can be achieved when transitioning from IOPS mode to Macro mode.

### 4.1.6 Key issue 2-6 on support MBMS in IOPS

#### 4.1.6.1 Description

eMBMS is an important feature for mission critical service to improve transmission efficiency. The eMBMS principle that an eNB is served by a single MCE and the different MCE deployments (i.e., distributed MCE architecture and centralized) in 3GPP TS 36.300 may impact the eMBMS usage in IOPS MC system.

IOPS MC system is based on IOPS network. The support of eMBMS is up to local operator policy and configuration as indicated in TS 23.401 :

*'The support by IOPS network entities of S1-flex and/or eMBMS is up to local operator policy and configuration.'*

Further study is needed:

- How to support MBMS feature in IOPS network;

- How the MCE deployments will impact the eMBMS usage in IOPS MC system; and

- How to minimize the delay in setting up eMBMS bearer when transitioning to IOPS.

### 4.1.7 Key issue 2-7 on determining a list of MC users connected to the IOPS MC system

#### 4.1.7.1 Description

When the IOPS operation is initiated due to a backhaul failure, it becomes a key issue for the MC users being served by the IOPS system to get informed about which other MC users are also registered within the IOPS system. For the implementation of a MC service system connected to the IOPS system, the MC users within the same MC service group can get informed about the affiliation status of others MC users in the group. However, it may not be possible for an MC service user to determine which other MC service users are also registered to the IOPS MC system during the IOPS operation, e.g. a list of users which have indicated that their registration status cannot be shared with other users in IOPS.

As described in the IOPS requirements in TS 22.346, the IOPS system shall be capable of informing served MC users about which other MC users are also served by the IOPS system. Thus, the MC users are notified of which other MC users they may perform a MC service communication with.

Further study is needed to identify how to support determining a list of MC users connected to the IOPS MC system after a backhaul failure has occurred.

# 5 Architectural requirements

## 5.1 IOPS related requirements

This subclause defines the architectural and functional requirements related to MC services in IOPS mode.

[MCSAA-REQ-1] The following MCPTT features shall be supported in IOPS

- MCPTT group call

- MCPTT emergency call

- MCPTT private call

[MCSAA-REQ-2] The following MCData features shall be supported in IOPS

- MCData short data service

Editor's Note: The list of features may be updated in the future.

[MCSAA-REQ-3] The MC services shall be supported in IOPS with no backhaul connectivity.

NOTE: Annex K in TS 23.401 does not specify any deployment option with limited backhaul. IOPS with limited backhaul is therefore subject for further work in SA2.

# 6 Solutions

## 6.1 Solution 1: UE and user data synchronization

### 6.1.1 Description

This solution addresses part of key issue 2-1 MC system configuration data synchronization. In the MC service configuration procedure as described in 3GPP TS 23.280 [7] subclause 10.1, the UE retrieves the initial UE configuration after the bootstrap. After the user authentication, the UE retrieves:

- UE configuration

- MC service user profile configuration

- Group configuration

The solution described in this clause covers the above configuration data with one exception. The Group configuration that resides in the group management system is not synchronized with this solution.

It is assumed that the initial UE configuration (e.g. APN details) can be kept as is and that there is no need to synchronize this data with the IOPS MC system. The initial UE configuration is provisioned by offline methods over reference point CSC-11.

It is assumed that the UE configuration data (e.g. MCPTT server URI) is of static nature and can be synchronized at system start up or reboot operation.

The MC service user profile data is dynamic data (e.g. contact lists) and may be updated daily which makes the synchronization of the data a challenge.

This solution proposes to synchronize the MC service user profile with the current (or IOPS tagged) profile that is currently active and downloaded in the MC service client. The procedure in figure 6.1.1-1 updates the MC service user profile for the MC service user in the IOPS MC system.

With this solution the MC service client is used to provide synchronization of the user data stored in the primary configuration management server with the configuration management server in the IOPS MC system.

Pre-conditions:

- The user must be defined in the IOPS MC system.

- The MC service client is authenticated and authorized by the IOPS MC system.



Figure 6.1.1-1: MC service user updates MC service user profile data to the MC IOPS system

1. The configuration management client is triggered (e.g. by detecting an MC IOPS system) to store or update the MC service user profile data on the configuration management server in the MC IOPS system.

NOTE: Step 1 could be triggered by the configuration management server.

2. The configuration management client sends create or update MC service user profile data request to the configuration management server, which includes the MC service user profile data to be updated.

3. The configuration management server stores the received MC service user profile data.

4. The configuration management server sends update MC service user profile data response to the configuration management client to confirm the MC service user profile data update is complete.

To avoid user data conflicts between IOPS MC system and the primary MC system, changes to MC service user profiles should not be allowed during IOPS mode by the IOPS MC system.

There is one disadvantage of this solution. Some parameters in the MC service user profile are not known by the UE. It is proposed to not use these parameters in an IOPS MC system. In the current version of 3GPP TS 23.379 [9] the following parameters are not downloaded to the UE:

- User profile status

- Authorised to create and delete aliases of an MCPTT User and its associated user profiles.

- Maximum number of simultaneously received group calls (Nc5)

- Priority of the user for initiating/receiving calls

- Authorisation to create a group-broadcast group

- Authorisation to create a user-broadcast group

- Authorisation to provide location information to other MCPTT users on a call when talking

- Authorisation of an MCPTT user to request a list of which groups an MCPTT user has affiliated to

- Authorisation to change affiliated groups of other specified user(s)

- Authorisation to recommend to specified user(s) to affiliate to specific group(s)

- Authorisation to query whether MCPTT User is available for private calls

- Authorisation to restrict provision of private call set-up failure cause to the caller

- Authorisation of an MCPTT user to cancel an emergency alert on any MCPTT UE of any MCPTT user

- Authorisation for a MCPTT user to enable/disable an MCPTT user

- Authorisation for an MCPTT user to (permanently /temporarily) enable/disable a UE

- Authorisation to revoke permission to transmit

- Maximum number of simultaneous transmissions received in one group call for override (N7)

- Authorised to interrogate the functional alias(es) active for another MCPTT user

- Authorised to take over a functional alias from another MCPTT user

Editor's note: How to handle the above parameters is FFS.

### 6.1.2 Impacts on existing nodes and functionality

Editor's Note: Capture impacts on existing 3GPP nodes and functional elements.

### 6.1.3 Solution evaluation

This solution does not prevent offline synchronization between MCPTT user databases or configuration management systems in primary MC system and IOPS MC system. The IOPS MC system has to validate service requests made by the MC UE against configuration data provided by the MC UE, which is a security concern as the system cannot prove whether the MC UE is requesting a service to which it is entitled.

## 6.2 Solution 2: Functional model for IOPS based on a switchable standalone MC system

### 6.2.1 Description

One solution for the architecture of IOPS MC system is to deploy a standalone system that is in standby during normal operations. The functional model of the IOPS MC system is illustrated in figure 6.2.1-1. The functional model includes the necessary functional entities for MC services in IOPS. The description of each functional entities is found in 3GPP TS 23.379 [9], 3GPP TS 23.280 [7] and 3GPP TS 23.282 [8].



Figure 6.2.1-1: Functional model for an IOPS MC system during IOPS mode

The following parts have been removed in the IOPS MC system functional entities

- Migration management server

- Reference points to other MC services servers, group management server, configuration management server.

### 6.2.2 Solution evaluation

This solution would provide a minor deviation from the functional model in a primary MC system. A few functional entities and reference points can be removed since they are not needed in the IOPS MC system. User and service data synchronization must be performed in all nodes that include permanent data.

The storage of duplicate configuration and security parameters in the IOPS MC system may cause security concerns.

## 6.3 Solution 3: Functional model for IOPS based on an always-on partner MC system

### 6.3.1 Description

One solution for the architecture of IOPS MC system is to have a fully functional and active MC system used during normal operations as a partner system to which the users may migrate based on MC service provider policies. The functional model of the IOPS MC system is illustrated in figure 6.3.1-1. For simplicity some of the internal reference points are not illustrated in the figure.



Figure 6.3.1-1: Functional model for an IOPS MC system based on migration of users

In this functional model the users may be migrated based on the UE location and the MC service provider policy, and by that receive the MC services from the IOPS MC system. This takes place prior that the IOPS mode is triggered by backhaul failure.

### 6.3.2 Solution evaluation

This solution provides a minor deviation from the functional model in a primary MC system. A few functional entities and reference points can be removed since they are not needed in the IOPS MC system. The users using the IOPS MC system need to migrate to the IOPS MC system prior to the transition to IOPS mode. User and service data synchronization is limited to users that have migrated to the IOPS MC system prior to a backhaul failure. There may be an issue in providing service to users who are not configured in the IOPS MC system, or who have not migrated to the IOPS MC system prior to the backhaul failure as their configuration data will not be accessible during the backhaul failure. This solution is not the preferred solution in a nomadic deployment.

## 6.4 Solution 4: Functional model for IOPS MC system based on only IP connectivity

### 6.4.1 Description

#### 6.4.1.1 General

This solution addresses key issue 2-4. One functional model for an IOPS MC system is to only utilize the IP connectivity that the local EPS provides, and by that only provide that MC services from the UEs.

The functional model of the IOPS MC system based on only IP connectivity is based on the off-network functional model and it is illustrated in figure 6.4.1.1-1.



Figure 6.4.1.1-1: Functional model for an IOPS MC system based on only IP connectivity

In this functional model the users do not obtain the MC services from a local MC service server. The local EPS network only provide IP connectivity. The configuration management client and the group management client needs must retrieve the configuration from the configuration management server and the group management server over CSC-4 and CSC-2 while the users are connected to the primary MC system.

This functional model allows communication between the MC users via the IOPS system, where the MC services are provided by the MC service clients and the IOPS system only relays the IP traffic. On the application layer most of the off-network procedures could be reused or taken as a reference. This type of MC communication in IOPS is defined as the IOPS-based IP connectivity communication.

Editor's note: It is FFS to define which procedures and protocols are utilized for the IOPS-based IP connectivity communication

Therefore, as part of this solution, an IOPS MC connectivity status function is implemented to be connected to the local EPC of the IOPS system to support discovering all MC users being served by the IOPS system. This procedure is defined as the IOPS-based discovery procedure. Also, an IOPS packet distribution function is implemented together with the IOPS MC connectivity status function and with connectivity to the IOPS system to handle IP packets received from the MC UEs and targeting other MC UEs being served by the IOPS system. In other words, the IOPS packet distribution function supports the IOPS-based IP connectivity communication by performing the IP relaying. The IP packets to be relayed contain the MC service related application data such as signalling control data or application data (control and media) generated by the MC service clients based on the IOPS-based IP connectivity communication. Figure 6.4.1.1-2 depicts the two new application functional entities in the IOPS MC system to provide IP connectivity to the MC users being served by the system. These new functional entities and related procedures are described further below.



Figure 6.4.1.1-2 IOPS MC system based on only IP connectivity

#### 6.4.1.2 IOPS-based discovery procedure

The IOPS-based discovery procedure is based on the publication, subscription and notification of connectivity information.

Once the MC UEs are being served by the IOPS system, the MC service clients initiates the discovery procedure by publishing their connectivity information to the IOPS MC connectivity status function. It is assumed that the IOPS MC connectivity status function also includes mechanisms to authenticate and authorize the MC users to register to the IOPS MC system.

The connectivity information may include some of the MC service configuration data available in the MC service clients when the IOPS mode of operation is initiated. For instance, if a MC user intends to utilize the MCPTT service while connected to the IOPS system, the connectivity information may include the following parameters (described in TS 23.379 Annex A.3 and TS 23.280 Annex A.4): MCPTT user identity (MCPTT ID), list of off-network MCPTT groups for use by an MCPTT user (MCPTT Group ID(s)), and ProSe group IP multicast address per MCPTT Group ID. Also, the connectivity information includes the IP address assigned to the MC UE by the local EPC for the IOPS-based IP connectivity communication (to be based on the IOPS APN). Furthermore, the connectivity information may include a parameter to indicate if the MC user connectivity information is available or not to be shared with other MC users connected to the IOPS system.

Upon reception of the publish requests, the IOPS MC connectivity status function stores the MC user connectivity information and defines the associated MC users as discovered, i.e. MC users that can be reached by other MC users via the IOPS system. How the received parameters within the connectivity information are managed by the IOPS MC connectivity status function is implementation specific.

When the MC users are discovered by the IOPS MC connectivity status function, the MC users subscribe to be notified about the connectivity status of other relevant discovered MC users. Relevant MC users can be other MC users connected to the IOPS system or a sub-set of users, e.g., other users which are within the list of users who can be called in private call or users which belong to the same MC service group.

Based on the received connectivity information, when the IOPS MC connectivity status function identifies that MC users associated to received subscriptions are discovered within the IOPS system, the IOPS MC connectivity status function notifies the MC users about the connectivity status of their relevant MC users, respectively. The connectivity status indicates if the relevant MC users are connected or not to the IOPS system and it provides information about how to establish an IOPS-based IP connectivity communication with other relevant MC users, e.g. the related IP address to communicate with another specific MC user.

The IOPS MC connectivity status function may periodically request to the discovered MC users to publish their connectivity status. Hence, the IOPS MC connectivity status function is aware of connectivity status changes of the discovered MC users and can notify the MC users with active subscriptions about these changes, respectively.

Figure 6.4.1.2-1 below describes the IOPS-based discovery procedure considering, as an example, two users, MC user 1 (UE1) and MC user 2 (UE2), where the MC UEs are attached and being served by the IOPS system. The MC users publish their connectivity information and the MC user 1 subscribes to receive notifications about the MC user 2 connectivity status.



Figure 6.4.1.2-1: IOPS-based discovery procedure

1. After the MC UEs are attached and being served by the IOPS system, the MC service clients initiate the IOPS-based discovery procedure

2. The MC user 1 at the MC service client 1 (2a) and the MC user 2 at the MC service client 2 (2b) publish their connectivity information to the IOPS MC connectivity status function

3. The IOPS MC connectivity status function stores the connectivity information of each MC user and defines the MC users as discovered

4. The IOPS MC connectivity status function may confirm to the MC service clients the reception of the publish requests.

5. The MC user 1 defines the MC user 2 as a relevant MC user, e.g. because the MC user 2 is within the MC user 1's list of users who can be called in private call, and subscribes to be notified about the connectivity status of the MC user 2.

6. The IOPS MC connectivity status function activates the subscription for the MC user 1.

7. The IOPS MC connectivity status function may confirm to the MC service client 1 the reception of the subscription request.

8. The IOPS MC connectivity status function, based on the received connectivity information, notifies the MC service client 1 about the connectivity status of the MC user 2. The connectivity status indicates that the MC user 2 is connected to the IOPS system and it contains information about how to establish an IOPS-based IP connectivity communication, e.g. the related IP address to communicate with the MC user 2.

9. The MC service client 1 notifies the MC user 1 about the connectivity status of the MC user 2.

10. The MC service client 1 may confirm to the IOPS MC connectivity status function the reception of the notification message.

#### 6.4.1.3 IOPS-based IP connectivity communication

In order to transmit the IP packets via the IOPS system, the MC service clients operating on the MC UEs implement for the transmission of the IP packets (containing the MC service related application data such as signalling control data or application data) an IP layer supporting IP encapsulation within IP (IETF RFC 2003), i.e. the IP packets are encapsulated with an inner IP header and an outer IP header. The inner IP header includes as IP address destination the related IP address of the targeted MC users(s). For the case of, e.g., a private call the related IP address destination is received within the notification message related to the relevant MC user. For the case of, e.g., a group call the related IP address destination to be utilized may be the pre-configured ProSe Group IP multicast address associated to the respective MC service group ID. On the other hand, the outer IP header includes as IP address destination the IP address of the IOPS packet distribution function. The MC UEs may be either pre-configured with the IP address of the IOPS packet distribution function for the IOPS operation or it may also be included in the notification messages as part of the discovery procedure.

The outgoing IP packets are sent to the MC UE's lower layers to be transmitted via the IOPS system to the IOPS packet distribution function for IP relaying. Figure 6.4.1.3-1 depicts the IP encapsulation of the application data for the IOPS-based IP connectivity communication.



Figure 6.4.1.3-1 MC UE's IP encapsulation of application data for the IOPS-based IP connectivity communication

When the IOPS packet distribution function receives the IP packets for relaying, it decapsulates them to get the IP packet containing the inner IP header, i.e. the related IP address of the targeted MC user(s). The IOPS packet distribution function resolves if that IP address destination is related to a Group IP multicast address (i.e. related to a MC service group ID) or to a unicast IP address (i.e. related to, e.g., a called MC user in a private call). Thus, and based on information stored in the IOPS MC connectivity status function, the packet distribution function transmits/relays the IP packets to the targeted MC UE(s) via the local EPS.

Editor's note: How the IOPS packet distribution function manages and relays the IP packets targeting a group of MC users is FFS

In the following, two examples are presented to describe the IOPS-based IP connectivity communication. The first example depicted in Figure 6.4.1.3-2 is the case of a MCPTT private call between two MC users (MC user 1 and MC user 2). The second example depicted in Figure 6.4.1.3-3 is the case of a MCPTT group call between three users (MC user 1, MC user 2, and MC user 3). The MC users are assumed to be defined as relevant to each other, e.g. the MC users belong to the same MC service group ID or are within the list of users who can be called in a private call.

For both examples, it is assumed that the MC UEs are being served by the IOPS system, the MC users have already performed the IOPS-based discovery procedure with the IOPS MC connectivity status function and the MC users support the IOPS-based IP connectivity communication. This means, the MC users have been already notified about the connectivity status of the other relevant discovered MC users within the IOPS system.



Figure 6.4.1.3-2 IOPS-based IP connectivity communication – MCPTT Private Call example

1. The MC user 1 at the MCPTT client 1 (operating on the MC UE 1) would like to initiate an MCPTT private call to the MC user 2 at the MCPTT client 2 (operating on MC UE 2).

2. The MCPTT client 1 sends a call setup request towards the MCPTT client 2. The call setup request is based on the procedures to be defined for the IOPS-based IP connectivity communication. For that, at the MC UE 1, the IP encapsulation within IP procedure is performed and the IP packets are sent to the MC UE 1's lower layers to be transmitted via the IOPS system to the IOPS packet distribution function.

3. The IOPS packet distribution function receives the IP packets from the IOPS system and performs the IP decapsulation. The IOPS packet distribution function resolves that the IP address destination is a unicast IP address of other MC UE within the IOPS system, i.e. MC UE 2.

4. The IOPS packet distribution function relays the IP packets related to the call setup request via the IOPS system towards the MC UE 2.

5. The MCPTT client 2 notifies the MC user 2 about the incoming private call.

6. The receiving MCPTT client 2 accepts the private call and a call setup response indicating the successful call establishment is sent to the MCPTT client 1. As described in step 2, the MC UE 2 also transmits the response IP packets via the IOPS system to the IOPS packet distribution function.

7. As described in step 3, the IOPS packet distribution function resolves that the IP address destination is a unicast IP address of other MC UE within the IOPS system, i.e. MC UE 1.

8. The IOPS packet distribution function relays the IP packets related to the call setup response via the IOPS system towards the MC UE 1.

9. The MCPTT client 1 and the MCPTT client 2 have successfully established the communication media plane based on the IOPS-based IP connectivity communication, i.e. all media plane data are also transmitted via the IOPS system and the IOPS packet distribution function.

10 It is assumed that the call has ended. Therefore, any of the MC users initiates a private call release based on the procedures to be defined for the IOPS-based IP connectivity communication. The MCPTT client 1 and the MCPTT client 2 release all associated media plane resources.



Figure 6.4.1.3-3 IOPS-based IP connectivity communication – MCPTT Group Call example

1. The MC user 1 at the MCPTT client 1 (operating on the MC UE 1) would like to initiate a group call with the MCPTT group, i.e. a group call targeting the MC user 2 at the MCPTT client 2 (operating on MC UE 2) and the MC user 3 at the MCPTT client 3 (operating on MC UE 3).

2. The MCPTT client 1 as the group call originator sends a group call announcement to the MCPTT group. The group call announcement is based on the procedures to be defined for the IOPS-based IP connectivity communication. For that, at the MC UE 1, the IP encapsulation within IP procedure is performed and the IP packets are sent to the MC UE 1's lower layers to be transmitted via the IOPS system to the IOPS packet distribution function.

3. The IOPS packet distribution function receives the IP packets from the IOPS system and performs the IP decapsulation. The IOPS packet distribution function resolves that the IP address destination is a Group IP address involving other discovered MC users within the IOPS system.

4. The IOPS packet distribution function relays the IP packets related to the group call announcement via the IOPS system towards all the other related MC users within the MCPTT group, i.e. the MC UE 2 and MC UE 3.

5. The MCPTT clients notify the MC users, respectively, about the incoming group call announcement.

6. The MCPTT clients 2 and 3 send the group call response to the MCPTT group. As described in step 2, the MC UEs also transmit the response packets via the IOPS system to the IOPS packet distribution function.

7. As described in step 3, the IOPS packet distribution function resolves that the IP address destination is a Group IP multicast address involving other MC users within the IOPS system.

8. The IOPS packet distribution function relays the IP packets related to the group call responses via the IOPS system towards all the other related MC users within the MCPTT group, i.e. the MC UE 1, MC UE 2 and MC UE 3, respectively.

9. The MCPTT clients have successfully established the communication media plane based on the IOPS-based IP connectivity communication, i.e. all media plane data are also transmitted via the IOPS system and the IOPS packet distribution function.

10 It is assumed that any of the users initiates the termination of the ongoing group call release based on the procedures to be defined for the IOPS-based IP connectivity communication. The MCPTT clients release all associated media plane resources.

### 6.4.2 Impacts on existing nodes and functionality

The reference points, procedures and protocols to be utilized for the IOPS-based discovery procedure and the IOPS-based IP connectivity communication need to be specified.

### 6.4.3 Solution evaluation

This solution provides a minimal deployment in each IOPS MC system. The IOPS MC system only requires that the IOPS-capable eNB(s) are connected to a local EPC, providing connectivity to the IOPS MC connectivity status function and packet distribution function. Challenges related to security requirements and data synchronization between the IOPS system and the primary MC system is by this functional mode minimized. The solution requires that all MC service clients are pre-provisioned with necessary MC service configuration and group configuration. This solution provides considerably better coverage and capacity when the user communication is based on the IOPS EPS IP connectivity compared to an off-network communication utilizing ProSe. Furthermore, a lower operational complexity can be achieved by the implementation of an IOPS MC connectivity status function and a packet distribution function compared to supporting an on-network based MC service server over an IOPS system. This considering that there is no need for synchronization of data between the central MC service server and all distributed MC servers over IOPS systems.

On the other hand, which procedures and protocols are utilized for the IOPS-based IP connectivity communication are FFS and require their specification.

## 6.5 Solution 5: Functional model for IOPS based on an always-on participating server

### 6.5.1 Description

This solution addresses key issue 2-4. One architectural solution for an IOPS MC system is to have a fully functional and active MC system used during normal operations. In the IOPS MC system the MC service server only execute the participating role during normal operating conditions and the primary MC system execute the controlling role. When the connection between the IOPS MC system and the primary system breaks the IOPS MC system execute both participating and controlling role of the MC service server.

Figure 6.5.1-1 below illustrates the deployment where several MC service servers assigned the participating role within one MC system are used for multiple UE based on their location. When the backhaul failure occurs, the IOPS MC system performs both the participating and controlling function.



Figure 6.5.1-1: IOPS MC system providing the participating function

The functional model of the IOPS MC system is illustrated in figure 6.5.1-2. For simplicity some of the internal reference points are not illustrated in the figure.



Figure 6.5.1-2: Functional model for an IOPS MC system based on always on participating server

In this functional model the users may be transferred to the IOPS MC system and actively use the MC service server's participating function. This trigger to transfer the users may be based on the UE location and the MC service provider policy, and by that receive part of the MC services from the IOPS MC system. This takes place prior that the IOPS mode is triggered by backhaul failure.

In the normal operation i.e. the backhaul transmission works, the common services core in the IOPS MC system is not used, instead the MC service client and the MC service server in the IOPS MC system is connected to the common services core in the primary MC system. The common services core still needs to be kept in sync with the primary MC system's common service core. When there is a backhaul failure the common services core in the IOPS MC system is used instead.

### 6.5.2 Solution evaluation

This solution provides a minor deviation from the functional model in a primary MC system. A few functional entities and reference points can be removed since they are not needed in the IOPS MC system. The users using the IOPS MC system need to switch to use the participating function of the MC service server in the IOPS MC system prior to the transition to IOPS mode. User and service data synchronization is limited to users that are using the IOPS MC system prior to a backhaul failure. There may be an issue in providing service to users who have not been transferred to the IOPS MC system prior to the backhaul failure as their configuration data will not be accessible during the backhaul failure. For these users there must be another data synchronization solution in place prior these users may enjoy MC services in IOPS mode.

This solution is not the preferred solution in a nomadic deployment.

## 6.6 Solution 6: Procedure for switching from the primary MC system to an IOPS MC system

### 6.6.1 Description

This solution address key issue 2-3. The solution utilizes the architecture defined in solution 5. In the procedure defined in this subclause the MC service client is triggered to re-register to the IOPS MC system and use the participating function in the MC service server in the IOPS MC system and the controlling function in the MC service server in the primary MC system.

### 6.6.2 Procedure

Figure 6.6.2-1 below specify the procedure for switching an MC service client from the primary MC system to the IOPS MC system. It requests the user to re-register in the IOPS MC system, while keeping part of the functionality (the controlling function) in the primary MC system.

Pre-conditions:

- The MC service client is authenticated and authorized by the primary MC system.

- The MC service client must be registered in the primary MC system.

- The MC service client has affiliated to one or several MC service groups.



Figure 6.6.2-1: Switching from the primary MC system to an IOPS MC system.

1. Group communication is handled by the primary MC system solely.

2. The MC client or the MC service server in the primary MC system detects that the MC client is in proximity of an IOPS MC system. How this is detected is implementation specific.

NOTE 1: Step 2 could be triggered by detecting that the cell that the UE is currently attached to is IOPS capable or that the MC service server knows that a neighbouring cell to the currently attached cell is IOPS capable.

3. In the scenario that the MC service server in the primary MC system decides that the MC services client shall be transferred to the IOPS MC system, the MC service server sends a re-registration request to the MC service client.

4. The MC service client performs the authentication and registration procedure as defined in 3GPP TS 23.280 [7].

NOTE 2: Step 4 causes service interruption and is therefore preferably avoided during active communication.

5. The MC service client affiliates to the MC service groups of interest, that request for affiliation is forwarded to the controlling function in the MC service server both in the IOPS MC system and the primary MC system.

6. Group communication is handled by the participating function in the IOPS MC system and the controlling function in the primary MC system.

7. The connectivity between the IOPS MC system and the primary MC system breaks.

8. Group communication is handled by the IOPS MC system solely. When the connectivity between the IOPS MC system and primary MC system is restored the group communication may continue, utilizing the primary MC systems controlling function. In this case any group affiliations that was done during IOPS mode must be forwarded to the primary MC system's MC service server.

Editor's note: It is FFS how the MC client switches from the participating function in the IOPS MC system to the participating function in the primary MC system or another IOPS MC system when the MC service client moves to area which is outside of proximity of current IOPS MC system.

### 6.6.3 Solution evaluation

This solution provides an efficient way to transfer ongoing calls from a primary MC system to an IOPS MC system when there is a failure in the connectivity between the IOPS MC system and the primary MC system.

This solution will utilize the existing stage-2 and stage-3 procedures for call setup procedures floor control for procedures involving one single system. The solution does not need to use the more complex procedures involving multiple MC service servers.

Users that has not been transferred to the IOPS MC system prior the failure needs to perform the authentication procedures (according to 3GPP TS 23.280 [7]) before accessing the service.

## 6.7 Solution 7: IOPS notification to MC UEs

### 6.7.1 Description

This solution addresses key issue 2-3 in how to optimize the user experience when MC UEs are switching to and from an IOPS MC system. An IOPS MC system does not have any connectivity to the primary MC system and therefore it cannot inform users that are not in the coverage of the IOPS system or even other MC system about the existence of the IOPS MC system. Since MC users are moving around and may enter or leave the IOPS system, the user experience will be unpredictable in terms of group constellations and delays during the switching time from the primary MC system served by one PLMN id to the IOPS MC system served by another PLMN id.

The procedure defined in this solution provides a notification to users that are likely to enter the IOPS MC system, which can improve the switching time and also give an indication to the user that the current active users in a group is impacted by the presence of the local IOPS MC system.

Preconditions:

- There is an IOPS MC system active and the neighbouring cells to the IOPS MC system is part of the primary MC system.

- The user has been defined in and registered to the IOPS MC system.

- The MC service client was authenticated and authorized by the IOPS MC system.



Figure 6.7.1-1: IOPS notification procedure to MC UEs in proximity of the IOPS MC system

1. Group communication is handled by the IOPS MC system.

2. The MC service client moves out of the coverage of the IOPS MC system and enters the primary MC system.

3. The MC service client sends a message to the primary MC system to inform the primary MC system about the existence of the IOPS MC system in the area. This message may also include geographical information, PLMN IDs, frequency bands and addresses to the local MC service servers.

4. The primary MC server may use the received information to take measures to optimize the provided MC service based on the changed conditions.

5. The primary MC system sends a message to all MC service clients in proximity of the IOPS MCS system to notify of the existence of a system. It may also include information that will improve the switching time when new MC UE's are moving into the MC IOPS system. This information may be e.g. geographical area / identified cells, IOPS users and groups, identified service degradation, PLMN IDs, frequency bands and addresses to the local MC service servers – the most important is dynamic information that else cannot be known by the Primary MC system. This message can preferably be sent on an MBMS bearer.

NOTE: Some parameters including PLMN ID may already be known by configuration

### 6.7.2 Impacts on existing nodes and functionality

Editor's Note: Capture impacts on existing 3GPP nodes and functional elements.

### 6.7.3 Solution evaluation

This contribution presents a solution for discovering that there is an active IOPS system operational. Based on this both the centralized MC service server and the MC service clients may take measures to provide a better user experience for users and better system performance. With knowledge of the IOPS situation and key parameters clients can make better mobility decisions between the centralized system and the IOPS system. The IOPS situation can also be notified to the end user, giving the end user an opportunity to actively move to or from the IOPS covered area based on increased situational awareness.

## 6.8 Solution 8: MC service client configuration for IOPS

### 6.8.1 Description

This solution addresses Key Issue 2-2 on how to prepare an MC service client for receiving an IOPS provided MC service.

An IOPS solution, according to Annex K in TS 23.401 [10] has a dedicated PLMN identity.

Procedures for retrieval of initial MC service UE configuration data, as specified in TS 23.280 [7] Annex A.6, can be re-used. The MC service UE is provided with initial UE configuration via a bootstrap procedure that provides the MC service UE's with critical information needed to connect to the MC system, as specified in TS 23.280 [7], subclause 10.1.1.1. This configuration includes HPLMN ID, an optional list of VPLMN IDs, APN, server URIs etc. The HPLMN parameter should be extended to a list of HPLMNs to support IOPS PLMN IDs.

The MC service client can then retrieve MC service UE Configuration according to TS 23.280 [7], subclause 10.1.3.

### 6.8.2 Solution evaluation

This solution is to a large extent already supported by existing specifications, efficiently reducing the complexity. The solution is dependent on that UE configuration data has ben successfully synchronized to the IOPS MC System (Key Issue 2-1). Since Initial UE configuration will be the same regardless if registering to the Primary MC system or an IOPS MC system this means that APN, server URIs etc needs to be the same in these systems.

## 6.9 Solution 9: Functionality for determining the MC user registration status in IOPS

### 6.9.1 Description

This solution addresses the key issue 2-7 on determining a list of MC users connected to the IOPS MC system when a backhaul failure has occurred. For that, one solution for the architecture of the IOPS MC system is to have a functionality in the IOPS MC system to manage dynamic data related to the registration status of MC users being served by the IOPS MC system.

The registration status function is implemented within the IOPS MC service system to provide mechanisms for the MC users being served by the IOPS MC system to query about which other MC users, or whether a particular MC user, are also registered to the IOPS MC system. Since an IOPS system provides local connectivity to only MC users, any MC user may be authorized to make such a query while connected to the IOPS MC system.

The MC service user profile may include new parameters to indicate if an MC user is authorized to query about the registration status of other MC users on the IOPS system as well as to indicate if the MC user registration status on the IOPS MC system is available or not to other MC users making such a query. For the later case, an MC user may publish to the IOPS MC system if the MC user's registration status becomes available or not to other users.

As the IOPS MC system may not identify when an MC user has left the IOPS system coverage area, the MC users may be requested to periodically publish that they are within the IOPS system. For that, the MC users may periodically publish that their registration status on the IOPS system is available to other MC users. Thus, the IOPS MC system can maintain the registration status of the MC users updated.

MC users which are interested to get informed about the registration status of other MC user(s) on the IOPS MC system subscribe to receive notifications of users which are relevant to them. MC users may be interested to subscribe to receive the registration status of all users connected to the IOPS MC system or just a sub-set of users, e.g. users which are within the list of users who can be called in private call or for users which belong to the same MC service group.

The MC users with active subscriptions receive the registration status of their relevant MC users via notification messages. These notifications can be sent by the IOPS MC system based on different triggers, e.g. any registration status change of the relevant MC users or as periodic notification messages defined by the IOPS MC system. For instance, when a particular relevant MC user is not anymore registered to the IOPS MC system, the IOPS MC system notifies all MC users with active subscriptions associated to that particular relevant MC user.

Figure 6.9.1-2 depicts an example of an IOPS MC system providing MCPTT services and supporting the registration status function. In this example, it is assumed that the registration status function is implemented as part of the MCPTT server. Also, the MC user 1 at the MCPTT client 1 defines the MC user 2 at the MCPTT client 2 as a relevant MC user, assuming that the MC user 2 is within the list of users who can be called via an MCPTT private call by the MC user 1.



Figure 6.9.1-2: Publication, subscription and notification for determining the MC user registration status of MC users on the IOPS MC system

1. The MC users at the MCPTT clients are registered to the IOPS MC system for the MCPTT service.

NOTE 1: The MC users may publish if their registration status on the IOPS MC system is available or not to other MC users.

2. MC user 1 defines the MC user 2 as a relevant MC user.

3. MC user 1 at the MCPTT client 2 sends a SUBSCRIBE request to the IOPS MC system to receive registration status notifications about the MC user 2.

4. The IOPS MC system may confirm the subscription request.

5. The IOPS MC system sends a NOTIFY message to the MC user 1 with the registration status of the MC user 2.

6. The MCPTT client 1 notifies the MC user 1 about the registration status of the MC user 2. Thereby, the MC user 1 knows that MC user 2 is within the IOPS system.

7. The MCPTT client 1 may confirm to the IOPS MC system the reception of the notification message.

8. The MC user 2 becomes disconnected from the IOPS MC system, e.g. because the MC UE 2 where the MC user 2 at the MCPTT client 2 is operating on, has left the IOPS system.

9. The IOPS MC system sends a NOTIFY message to the MC user 1 informing that the registration status of the MC user 2 has changed to disconnected.

10 The MCPTT client 1 notifies the MC user 1 about the registration status change of the MC user 2. Thereby, the MC user 1 knows that MC user 2 is not anymore within the IOPS system.

NOTE 2: Based on the MC user 1 subscription, the MC user 1 might get notified once the MC user 2 is again connected to the IOPS system.

11. The MCPTT client 1 may confirm to the IOPS MC system the reception of the notification message.

12. The MC user 2 at the MCPTT client 2 is again registered to the IOPS MC system.

13. The IOPS MC system sends a NOTIFY message to the MC user 1 informing that the registration status of the MC user 2 has changed to registered.

14. The MCPTT client 1 notifies the MC user 1 about the registration status change of the MC user 2. Thereby, the MC user 1 knows that MC user 2 is again within the IOPS system.

15 The MCPTT client 1 may confirm to the IOPS MC system the reception of the notification message.

16. As the MC user 1 is aware that it can reach out to the MC user 2, the MC user 1 initiates and establishes an MCPTT private call with the MC user 2.

### 6.9.2 Solution evaluation

This solution provides a mechanism to handle dynamic data related to the registration status of the MC users on the IOPS MC system. Thus, the MC users registered to the IOPS MC system can query the registration status of other MC users connected to the IOPS MC system.

This solution proposes that all MC users which are already registered to the IOPS MC service system may be authorized to query the registration status of other MC users within the IOPS system. Also, the MC service user profile may include new parameters to indicate if an MC user is authorized to query about the registration status of other MC users on the IOPS system as well as to indicate if the MC user registration status on the IOPS MC system is available or not to other MC users making such a query. For the later, the MC user may publish if its registration status becomes or not available to other MC users. Furthermore, MC users can subscribe to receive notification about the registration status of other MC users connected to the IOPS MC system.

# 7 Overall evaluation

## 7.1 General

The following subclauses contain an overall evaluation of the solutions presented in this technical report, and their applicability to the identified key issues.

- Subclause 7.2 provides an evaluation of the functional model solutions for the MC service architecture to be used during the IOPS mode of operation; and

- Subclause 7.3 provides an evaluation of the introduced solutions for the key issues including the impact on other working groups that will need consideration.

## 7.2 Architecture evaluation

The functional model solutions studied in this technical report are based on the on-network and off-network functional models described in 3GPP TS 23.280. The functional model solutions based on the on-network functional model include having a fully functional IOPS MC system, which can be either in standby (standalone system) or active (acting as a partner system) during normal operation. On the other hand, the functional model solution based on the off-network functional model is a model where the IOPS MC system only provides IP connectivity to the served MC users.

A summary of the functional model solutions studied in this technical report are listed in table 7.2-1.

Table 7.2-1: Architecture evaluation – Functional model solutions in IOPS

| Architecture solution | Applicable key issues  (subclause reference) | Evaluation  (subclause reference) | Dependency on other working groups |
| --- | --- | --- | --- |
| Solution 2 - Functional model for IOPS based on a switchable standalone MC system | Key issue specified in subclauses: 4.1.4 (Key issue 2-4) | 6.2.2 | (see NOTE 1) |
| Solution 3 - Functional model for IOPS based on an always-on partner MC system | Key issue specified in subclauses: 4.1.4 (Key issue 2-4) | 6.3.2 | (see NOTE 1) |
| Solution 4 - Functional model for IOPS MC system based on only IP connectivity | Key issue specified in subclauses: 4.1.4 (Key issue 2-4) | 6.4.3 | (see NOTE 1)  (see NOTE 2) |
| Solution 5 - Functional model for IOPS based on an always-on participating server | Key issue specified in subclauses: 4.1.4 (Key issue 2-4) | 6.5.2 | (see NOTE 1) |
| NOTE 1: This solution shall include mechanisms to authorize and authenticate MC users to be served by the IOPS MC system. Such mechanisms need to be addressed and defined by SA3.  NOTE 2: This solution includes new entities in the application architecture. The definition of the EPC interfaces to be used for these new entities might involve other working groups, e.g. SA2. | | | |

The functional model of solutions 2, 3, and 5 are based on the on-network functional model. These solutions require that all available IOPS MC systems maintain a fully user and service data synchronization with the primary MC system before the occurrence of a backhaul failure. As described in the key issue 2-1, the user and service configuration data synchronization between the (on-network based) IOPS MC systems and the primary MC system is relevant to support MC services during the IOPS mode of operation. The implementation of such a mechanism, however, implies a high operational complexity to guarantee that all the available IOPS MC system within the network are fully synchronized with the primary MC system before a backhaul failure. Besides, it involves the distribution and storage of all service and user related data in all available IOPS MC systems within a network which may involve further security issues.

The functional model of solution 4 is based on the off-network functional model. This MC-service-server-less functional model allows communication between the MC users via the IOPS MC system, where the MC services are provided by the MC service clients and the IOPS system only relays the IP traffic. For that, two (new) functional entities in the IOPS MC system are required to provide the IP connectivity functionality to the served MC users. This solution does not require configuration data synchronization between the primary MC system and all available IOPS MC systems. Therefore, a lower operational complexity can be achieved and security issues can also be mitigated.

## 7.3 Key issue and solution evaluation

All the key issues and solutions specified in this technical report are listed in table 7.3-1. It includes the mapping of the key issues (clause 4) to the solutions and corresponding solution evaluations. Also, it lists the dependency on other working groups that need consideration during the Rel-17 normative phase.

Table 7.3-1: Key issue and solution evaluation

| Key issues | Solution | Evaluation  (subclause reference) | Dependency on other working groups |
| --- | --- | --- | --- |
| Key issue 2-1 - MC system configuration data synchronization | Solution 1 - UE and user data synchronization | 6.1.3 | None |
| Key issue 2-2 - MC service client configuration for IOPS | Solution 8 - MC service client configuration for IOPS | 6.8.2 | None |
| Key issue 2-3 - on how to handle an MC UE switching to/from an IOPS MC system | Solution 6 - Procedure for switching from the primary MC system to an IOPS MC system  Solution 7 - IOPS notification to MC UEs | 6.6.3, 6.7.3 | None |
| Key issue 2-4 - IOPS architecture | (see NOTE 1) |  |  |
| Key issue 2-5 - on ongoing communication continuity when backhaul is recovered | (see NOTE 2) |  |  |
| Key issue 2-6 - on support MBMS in IOPS | (see NOTE 3) |  |  |
| Key issue 2-7 - on determining a list of MC users connected to the IOPS MC system | Solution 9 - Functionality for determining the MC user registration status in IOPS | 6.9.2 | None |
| NOTE 1: The evaluation of the solutions related to key issue 2-4 is described in subclause 7.2.  NOTE 2: There was no solution addressing key issue 2-5. However, based on how the IOPS mode of operation is defined in 3GPP TS 23.401 Annex K, when the IOPS mode of operation ceases the MC UEs are moved to Idle mode. Therefore, the MC UEs are required to reselect the normal PLMN and attach again to the macro EPC. So, ongoing communication continuity cannot be achieved based on the current definition of the IOPS mode of operation.  NOTE 3: MBMS support in IOPS has not been addressed during this study. However, it can be addressed as part of the normative phase. | | | |

Solutions 7, 8 and 9 addressing key issues 2-3, 2-2 and 2-7, respectively, can be implemented for both on-network and off-network based IOPS MC systems.

Solution 1 addressing key issue 2-1 is based on an on-network functional model. As described in clause 6.1, this solution entails an issue about how an on-network based MC IOPS system can handle missing user and service parameters that are not available at the MC clients and required for a normal on-network operation. This means that the IOPS MC system cannot be fully based on the specified on-network procedures. Instead, new mechanisms need to be considered for the operation of the IOPS MC system under the situation of these missing parameters. This can be translated to a high standardization impact. Also, this can lead to a high implementation and operational complexity for an on-network based MC system being able to operate under normal operation as well as IOPS mode of operation.

Also, considering that an IOPS solution may include the availability and deployment of several IOPS MC systems within a network, the required footprint and complexity to implement and deploy on-network based IOPS MC systems will be much higher than off-network based IOPS MC systems.

On the other hand, as described in subclause 7.2, in an off-network based IOPS MC system, i.e. solution 4, the key issue 2-1 is mitigated. This requires, however, that the already specified off-network protocol and related procedures are enhanced, so that the off-network application can be used regardless which transport is utilized. Hence, the off-network application can be enabled to operate over different (3GPP and non-3GPP) IP-based transports, e.g. over LTE ProSe (as defined today), over the IOPS MC system (based on solution 4), and others (e.g. 5G).

# 8 Conclusions

This technical report fulfills the objectives of the study on mission critical services access aspects (MCSAA), including the following:

1) Identification of key issues (clause 4) and architecture requirements (clause 5).

2) Identification of architectural requirements.

3) Application architecture solutions and individual solutions (clause 6) addressing the key issues (clause 4).

4) Overall evaluation (clause 7) of the solutions.

The results from the study have identified the following observations:

- The implementation of a synchronization mechanism between all available IOPS MC systems and the primary MC system implies a high operational complexity.

- The need of service and user related data synchronization between all the IOPS MC systems and the primary MC system may represent further security issues.

- An off-network functional model based solution does not require configuration data synchronization between the primary MC system and all available IOPS MC systems. Also, it mitigates security issues.

- An on-network based IOPS MC system where the configuration data is provisioned by the MC service clients will need the specification of new procedures and mechanisms to operate under the situation of having missing required parameters. This can lead to a high implementation and operational complexity for an on-network based MC system being able to operate under normal operation as well as IOPS mode of operation.

- The required footprint and complexity to implement and deploy on-network based IOPS MC systems will be much higher than off-network based IOPS MC systems.

- The off-network application can be enhanced, so that they are enabled to operate over different (3GPP and non-3GPP) IP-based transports, e.g. over LTE ProSe (as defined today), over the IOPS MC system (based on solution 4), and others (e.g. 5G).

NOTE: The solutions identified in this study are based on the IOPS mode of operation described in 3GPP TS 23.401 Annex K. However, for the case of a backhaul failure the access network aspects, e.g. security aspects at the network layer, need to be further addressed.

The results from the study will be considered for the follow-up normative work in Release 17, as follows:

1) The support of MC services on IOPS will be based on an IOPS MC system functional model that does not require configuration data synchronization with the primary MC system.

2) The off-network based solution 4 (subclause 6.4) is the preferred option to be considered as the baseline functional model for the support of MC services during the IOPS mode of operation, including:

a. Enhancing, if required, the off-network application related procedures to enable them to operate over LTE ProSe (as today) as well as over IOPS.

3) Key issues (clause 4) and individual solutions (clause 6) will be considered, but not limited to, as candidate solutions for the support of MC services during the IOPS mode of operation.

The dependencies to other 3GPP groups have been identified in the overall evaluation (clause 7).

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2018-03 | SA6#22 |  |  |  |  | TR skeleton | 0.0.0 |
| 2018-03 | SA6#22 |  |  |  |  | TR Skeleton agreed in SA6#22: S6-180316  Implemented pCR approved in SA6#22: S6-180432, S6-180495 Editorial changes by rapporteur | 0.1.0 |
| 2018-04 | SA6#23 |  |  |  |  | Implemented pCR approved in SA6#23: S6-180664, S6-180704, S6-180705, S6-180717  Editorial changes by the rapporteur | 0.2.0 |
| 2018-05 | SA6#24 |  |  |  |  | Implemented pCR approved in SA6#24: S6-180901, S6-180902, S6-180962, S6-180963  Editorial changes by the rapporteur | 0.3.0 |
| 2018-07 | SA6#25 |  |  |  |  | Implemented pCR approved in SA6#25: S6-181189, S6-181254  Editorial changes by the rapporteur | 0.4.0 |
| 2018-10 | SA6#26 |  |  |  |  | Implemented pCRs approved in SA6#15: S6-181545, S6-181564, S6-181590  Editorial changes by the rapporteur | 0.5.0 |
| 2018-12 | SA6#27 |  |  |  |  | Implemented pCR approved in SA6#27: S6-181842 | 0.6.0 |
| 2018-12 | SA#82 | SP-181143 |  |  |  | Presentation for information at SA#82 | 1.0.0 |
| 2019-12 | SA6#28 |  |  |  |  | Implemented pCR approved in SA6#28: S6-190270 | 1.1.0 |
| 2019-03 | SA6#29 | S6-190516 |  |  |  | Approved pCR on IOPS discovery procedure | 1.2.0 |
| 2019-04 | SA6#30 |  |  |  |  | Implemented pCRs approved in SA6#30: S6-190574, S6-190731, S6-190732, S6-190733, S6-190735, S6-190870, S6-190871  Editorial changes by the rapporteur | 1.3.0 |
| 2019-05 | SA6#31 |  |  |  |  | Implemented pCRs approved in SA6#31: S6-191086, S6-191197, S6-191198.  Editorial changes by the rapporteur | 1.4.0 |
| 2019-05 | SA#84 | SP-190470 |  |  |  | Presentation for Approval at SA#84 | 2.0.0 |
| 2019-06 | SA#84 | SP-190470 |  |  |  | MCC Editorial update for publication after TSG SA approval (SA#84) | 16.0.0 |