3GPP TR 23.784 V16.0.0 (2019-06)

Technical Specification

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Study on discreet listening and logging

for mission critical services

(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 Specification 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

Int[ernet](./ernet%0Dhttp://www.3g)

[http://www.3g](./ernet%0Dhttp://www.3g)pp.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 [6](#__RefHeading___Toc11678088)

1 Scope [7](#__RefHeading___Toc11678089)

2 References [7](#__RefHeading___Toc11678090)

3 Definitions and abbreviations [7](#__RefHeading___Toc11678091)

3.1 Definitions [7](#__RefHeading___Toc11678092)

3.2 Abbreviations [8](#__RefHeading___Toc11678093)

4 Scenarios [8](#__RefHeading___Toc11678094)

4.1 General [8](#__RefHeading___Toc11678095)

4.2 Scenario 1: Discreet listening of MCPTT and MCVideo private calls [8](#__RefHeading___Toc11678096)

4.2.1 Scenario 1.1: Discreet listening of MCPTT and MCVideo private calls in same MC service server [8](#__RefHeading___Toc11678097)

4.2.2 Scenario 1.2: Discreet listening of MCPTT and MCVideo private calls with target receiving service from different MC service server [9](#__RefHeading___Toc11678098)

4.3 Scenario 2: Discreet listening of MCPTT and MCVideo group calls [10](#__RefHeading___Toc11678099)

4.4 Scenario 3: Discreet listening of MCVideo pull [11](#__RefHeading___Toc11678100)

4.4.1 Scenario 3.1: Discreet listening of one to one MCVideo pull [11](#__RefHeading___Toc11678101)

4.4.2 Scenario 3.2: Discreet listening of one from server MCVideo pull [12](#__RefHeading___Toc11678102)

4.5 Scenario 4: Discreet listening of MCVideo push [12](#__RefHeading___Toc11678103)

4.5.1 Scenario 4.1: Discreet listening of one to one MCVideo push [12](#__RefHeading___Toc11678104)

4.5.2 Scenario 4.2: Discreet listening of one to server MCVideo push [13](#__RefHeading___Toc11678105)

4.5.3 Scenario 4.3: Discreet listening of remotely initiated MCVideo push [13](#__RefHeading___Toc11678106)

4.6 Scenario 5: Discreet listening of MCData SDS [14](#__RefHeading___Toc11678107)

4.7 Scenario 6: Discreet listening of MCData file distribution [15](#__RefHeading___Toc11678108)

4.7.1 Scenario 6.1: Discreet listening of file upload and file download [15](#__RefHeading___Toc11678109)

4.7.2 Scenario 6.2: Discreet listening of one to one file distribution [15](#__RefHeading___Toc11678110)

4.8 Scenario 7: Logging scenarios [16](#__RefHeading___Toc11678111)

4.8.1 General [16](#__RefHeading___Toc11678112)

4.9 Scenario 8: Limitations on discreet listening due to regulatory constraints and operator security policies [17](#__RefHeading___Toc11678113)

4.9.1 Scenario 8.1: Private communication transmissions [17](#__RefHeading___Toc11678114)

4.9.2 Scenario 8.2: Group communication transmissions [17](#__RefHeading___Toc11678115)

5 Key Issues [18](#__RefHeading___Toc11678116)

5.1 Key Issue 1: Selection of MC service for discreet listening [18](#__RefHeading___Toc11678117)

5.2 Key issue 2: Group membership of authorized MC user for discreet listening [19](#__RefHeading___Toc11678118)

5.3 Key issue 3: Discreet listening for MCVideo push and pull and MCData file upload and download [19](#__RefHeading___Toc11678119)

5.4 Key issue 4: Discreet listening of end to end encrypted calls [20](#__RefHeading___Toc11678120)

5.5 Key issue 5: Logging and replay of end to end encrypted calls [20](#__RefHeading___Toc11678121)

5.6 Key issue 6: Source MC service server for discreet listening of user in group call [21](#__RefHeading___Toc11678122)

5.7 Key issue 7: Discreet listening and logging for interconnected MC system [21](#__RefHeading___Toc11678123)

5.8 Key issue 8: Discreet listening and logging for migrated MC service user [22](#__RefHeading___Toc11678124)

5.9 Key Issue 9: Discreet listening and logging for user receiving MC service on multiple devices [22](#__RefHeading___Toc11678125)

5.10 Key Issue 10: Logging of MC service users and MC service groups [23](#__RefHeading___Toc11678126)

5.11 Key Issue 11: Logging of MCData content server and message store services [23](#__RefHeading___Toc11678127)

5.12 Key Issue 12: Discreet listening of MCData content server and message store services [24](#__RefHeading___Toc11678128)

5.13 Key issue 13: Discreet listening towards an MC service group [24](#__RefHeading___Toc11678129)

5.14 Key Issue 14: Limitations on discreet listening due to regulatory constraints and operator security policies [24](#__RefHeading___Toc11678130)

6 Solutions [25](#__RefHeading___Toc11678131)

6.1 Solution 1: Functionality for discreet listening [25](#__RefHeading___Toc11678132)

6.1.1 Description [25](#__RefHeading___Toc11678133)

6.1.1.1 Functional model [25](#__RefHeading___Toc11678134)

6.1.1.2 Configuration [25](#__RefHeading___Toc11678135)

6.1.1.3 Procedures [26](#__RefHeading___Toc11678136)

6.1.1.3.1 General [26](#__RefHeading___Toc11678137)

6.1.1.3.2 Discreet listening invocation and revocation procedures [26](#__RefHeading___Toc11678138)

6.1.1.3.3 Provision of discreet listening content for private communications [26](#__RefHeading___Toc11678139)

6.1.1.3.4 Provision of discreet listening content for group communications [27](#__RefHeading___Toc11678140)

6.1.1.3.5 Information flows for discreet listening [28](#__RefHeading___Toc11678141)

6.1.2 Impacts on existing nodes and functionality [28](#__RefHeading___Toc11678142)

6.1.3 Solution Evaluation [28](#__RefHeading___Toc11678143)

6.2 Solution 2: Discreet listening of MCVideo push and pull [28](#__RefHeading___Toc11678144)

6.2.1 Description [28](#__RefHeading___Toc11678145)

6.2.1.1 Overview [28](#__RefHeading___Toc11678146)

6.2.1.2 Invocation [29](#__RefHeading___Toc11678147)

6.2.1.3 MCVideo push discreet listening procedure [29](#__RefHeading___Toc11678148)

6.2.1.4 MCVideo pull discreet listening procedure [30](#__RefHeading___Toc11678149)

6.2.1.5 Information flows for discreet listening of MCVideo push and pull [31](#__RefHeading___Toc11678150)

6.2.2 Impacts on existing nodes and functionality [31](#__RefHeading___Toc11678151)

6.2.3 Solution Evaluation [32](#__RefHeading___Toc11678152)

6.3 Solution 3: Functionality for on-network logging and replay [32](#__RefHeading___Toc11678153)

6.3.1 Description [32](#__RefHeading___Toc11678154)

6.3.1.1 Functional model [32](#__RefHeading___Toc11678155)

6.3.1.2 Configuration [34](#__RefHeading___Toc11678156)

6.3.1.3 Procedures [35](#__RefHeading___Toc11678157)

6.3.2 Impacts on existing nodes and functionality [36](#__RefHeading___Toc11678158)

6.3.3 Solution Evaluation [36](#__RefHeading___Toc11678159)

6.4 Solution 4: On-network logging for interconnection and migration [37](#__RefHeading___Toc11678160)

6.4.1 Description [37](#__RefHeading___Toc11678161)

6.4.1.1 General [37](#__RefHeading___Toc11678162)

6.4.1.2 Functional model [37](#__RefHeading___Toc11678163)

6.4.1.3 Configuration [38](#__RefHeading___Toc11678164)

6.4.1.3.1 General [38](#__RefHeading___Toc11678165)

6.4.1.3.2 Logging of group communications in partner system [38](#__RefHeading___Toc11678166)

6.4.1.3.3 Logging of individual communications – option 1 [39](#__RefHeading___Toc11678167)

6.4.1.3.4 Logging of individual communications – option 2 [39](#__RefHeading___Toc11678168)

6.4.1.3.5 Logging of individual communications – option 3 [39](#__RefHeading___Toc11678169)

6.4.1.4 Procedures [40](#__RefHeading___Toc11678170)

6.4.2 Impacts on existing nodes and functionality [40](#__RefHeading___Toc11678171)

6.4.3 Solution Evaluation [40](#__RefHeading___Toc11678172)

6.5 Solution 5: Discreet listening for interconnection and migration [40](#__RefHeading___Toc11678173)

6.5.1 Description [40](#__RefHeading___Toc11678174)

6.5.1.1 Functional model [40](#__RefHeading___Toc11678175)

6.5.1.2 Configuration [40](#__RefHeading___Toc11678176)

6.5.1.2.1 General [40](#__RefHeading___Toc11678177)

6.5.1.2.2 User profile authorization of discreet listening – option 1 [41](#__RefHeading___Toc11678178)

6.5.1.2.3 Sharing the user profile for authorized users – option 2 [41](#__RefHeading___Toc11678179)

6.5.1.2.4 New configuration table of authorized users – option 3 [42](#__RefHeading___Toc11678180)

6.5.1.3 Procedures [42](#__RefHeading___Toc11678181)

6.5.2 Impacts on existing nodes and functionality [42](#__RefHeading___Toc11678182)

6.5.3 Solution Evaluation [42](#__RefHeading___Toc11678183)

6.6 Solution 6: Discreet listening to an MCPTT group [43](#__RefHeading___Toc11678184)

6.6.1 Description [43](#__RefHeading___Toc11678185)

6.6.1.1 Overview [43](#__RefHeading___Toc11678186)

6.6.1.2 Configuration [43](#__RefHeading___Toc11678187)

6.6.1.3 Procedures [44](#__RefHeading___Toc11678188)

6.6.1.3.1 Discreet listening activation and deactivation [44](#__RefHeading___Toc11678189)

6.6.1.3.2 Provision of discreet listening to groups [44](#__RefHeading___Toc11678190)

6.6.1.3.3 Release discreet listening to groups [45](#__RefHeading___Toc11678191)

6.6.1.4 Information flows [46](#__RefHeading___Toc11678192)

6.6.2 Impacts on existing nodes and functionality [48](#__RefHeading___Toc11678193)

6.6.3 Solution Evaluation [48](#__RefHeading___Toc11678194)

6.7 Solution 7: Logging of MCData message store and MCData content server [48](#__RefHeading___Toc11678195)

6.7.1 Description [48](#__RefHeading___Toc11678196)

6.7.1.1 Overview [48](#__RefHeading___Toc11678197)

6.7.1.2 Logging of MCData message store services [48](#__RefHeading___Toc11678198)

6.7.1.3 Logging of MCData content server transactions [49](#__RefHeading___Toc11678199)

6.7.2 Impacts on existing nodes and functionality [50](#__RefHeading___Toc11678200)

6.7.3 Solution Evaluation [50](#__RefHeading___Toc11678201)

6.8 Solution 8: Discreet listening of MCData message store and MCData content server [50](#__RefHeading___Toc11678202)

6.8.1 Description [50](#__RefHeading___Toc11678203)

6.8.1.1 Overview [50](#__RefHeading___Toc11678204)

6.8.1.2 Discreet listening of MCData message store services [50](#__RefHeading___Toc11678205)

6.8.1.3 Discreet listening of MCData content server transactions [51](#__RefHeading___Toc11678206)

6.8.2 Impacts on existing nodes and functionality [52](#__RefHeading___Toc11678207)

6.8.3 Solution Evaluation [52](#__RefHeading___Toc11678208)

6.9 Solution 9: Functionality for discreet listening with regulatory constraints and operator security policies [52](#__RefHeading___Toc11678209)

6.9.1 Description [52](#__RefHeading___Toc11678210)

6.9.1.1 Functional model [52](#__RefHeading___Toc11678211)

6.9.1.2 Configuration [53](#__RefHeading___Toc11678212)

6.9.1.3 Procedures [53](#__RefHeading___Toc11678213)

6.9.1.3.1 General [53](#__RefHeading___Toc11678214)

6.9.1.3.2 Discreet listening invocation and revocation procedures [53](#__RefHeading___Toc11678215)

6.9.1.3.3 Provision of discreet listening content for private communications [54](#__RefHeading___Toc11678216)

6.9.1.3.4 Provision of discreet listening content for group communications [55](#__RefHeading___Toc11678217)

6.9.1.3.5 Information flows for discreet listening [55](#__RefHeading___Toc11678218)

6.9.2 Impacts on existing nodes and functionality [55](#__RefHeading___Toc11678219)

6.9.3 Solution Evaluation [56](#__RefHeading___Toc11678220)

6.10 Solution 10: Functionality for on-network logging and replay [56](#__RefHeading___Toc11678221)

6.10.1 Description [56](#__RefHeading___Toc11678222)

6.10.1.1 Functional model [56](#__RefHeading___Toc11678223)

6.10.1.2 Configuration [57](#__RefHeading___Toc11678224)

6.10.1.3 Procedures [57](#__RefHeading___Toc11678225)

6.10.2 Impacts on existing nodes and functionality [57](#__RefHeading___Toc11678226)

6.10.3 Solution Evaluation [58](#__RefHeading___Toc11678227)

7 Overall Evaluation [58](#__RefHeading___Toc11678228)

7.1 General [58](#__RefHeading___Toc11678229)

7.2 Solution evaluation [58](#__RefHeading___Toc11678230)

7.3 Key issues with security implications [62](#__RefHeading___Toc11678231)

8 Conclusions [62](#__RefHeading___Toc11678232)

Annex A: Reproduction of stage 1 requirements [62](#__RefHeading___Toc11678233)

A.1 Requirements for discreet listening [62](#__RefHeading___Toc11678234)

A.2 Requirements for recording and audit [63](#__RefHeading___Toc11678235)

Annex B (informative): Change history [64](#__RefHeading___Toc11678236)

# Foreword

This Technical Specification 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.

# 1 Scope

The present document studies solutions to satisfy the requirements for discreet listening and logging for mission critical services. It identifies enhancements to be included in the technical specifications for MCPTT, MCVideo, MCData and in the common functional architecture to support mission critical services. Requirements for this study are taken from the Stage 1 requirements, including 3GPP TS 22.280 [2], and 3GPP TS 22.281 [3].

# 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 22.280: "Mission Critical Services Common Requirements (MCCoRe)"

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

[4] 3GPP TS 22.179: "Mission Critical Push To Talk (MCPTT); Stage 1"

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

[6] 3GPP TS 33.180: "Security of the mission critical service"

[7] 3GPP TS 23.379: "Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2"

[8] 3GPP TS 23.281: "Functional architecture and information flows to support Mission Critical Video (MCVideo); Stage 2".

[9] 3GPP TS 23.282: "Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2".

[10] 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control; Protocol specification"

[11] 3GPP TS 24.281: "Mission Critical Video (MCVideo) signalling control; Protocol specification"

[12] 3GPP TS 24.282: "Mission Critical Data (MCData) signalling control; Protocol specification"

# 3 Definitions 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].

**Discreet listening:** A means for an authorized user to be provided with the communications of a target user, without any unauthorized user in the communications being aware.

**Migrated MC system:** The partner MC system to which an MC service user has migrated, and in which that migrated MC service user is receiving MC service.

**Security Domain**: A set of MC users who share common security requirements and policies for their communications.

## 3.2 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].

FD File Distribution

GMK Group Master Key

GMS Group Management Server

MC Mission Critical

SDS Short Data Service

# 4 Scenarios

## 4.1 General

The following subclauses describe scenarios that will arise from a request from an authorized MC user for discreet listening of the communications of a second MC user within the authority of the authorized MC user. Use cases for MCPTT, MCVideo and MCData are captured.

In each case, the authorized MC user will be presented with media which has originated from or is destined for the target MC user of the discreet listening request. If this media is protected by encryption and other security measures, the mechanism by which the actual content of the media is revealed to the authorized MC user is outside the scope of the present document.

## 4.2 Scenario 1: Discreet listening of MCPTT and MCVideo private calls

### 4.2.1 Scenario 1.1: Discreet listening of MCPTT and MCVideo private calls in same MC service server

This scenario describes the case where authorized MC user A requests discreet listening for communications involving MC user B where MC user A and MC user B are served by the same MC service server, MC service server A and MC service user B is within the authority of authorized MC user A. The scenario is illustrated in figure 4.2.1-1 below.



Figure 4.2.1-1: Discreet listening of MCPTT or MCVideo private call in single MC service server

The scenario consists of the following aspects:

- Authorized MC user A identifies MC user B as the target for discreet listening, and the request for discreet listening is sent by MC service client A to MC service server A, which verifies that MC user A is authorized to perform discreet listening on MC user B. This aspect takes place before any communications involving MC user B can be subject to discreet listening.

- MC user B places or receives an MCPTT or MCVideo private call to or from MC user C.

- MC service server A provides MC service client A with information concerning the initiation of the call, including the identity of MC user C, and also provides the media exchanged between the two parties in the call.

- When the private call completes, the call completion is also conveyed to MC service client A.

NOTE: The scenario also applies to emergency private calls.

### 4.2.2 Scenario 1.2: Discreet listening of MCPTT and MCVideo private calls with target receiving service from different MC service server

This scenario describes the case where authorized MC user A requests discreet listening for communications involving MC user B where MC service user B is within the authority of authorized MC user A and where MC user A and MC user B have different primary MC service servers, MC service servers A and B. The scenario is illustrated in figure 4.2.2-1 below.



Figure 4.2.2-1: Discreet listening of MCPTT or MCVideo private call with target served by different MC service servers

The scenario consists of the following aspects:

- Authorized MC user A identifies MC user B as the target for discreet listening, and the request for discreet listening is sent by MC service client A to MC service server A, which verifies that MC user A is authorized to perform discreet listening on MC user B. This aspect takes place before any communications involving MC user B can be subject to discreet listening.

- MC service server A identifies MC service server B as the primary MC service server for MC user B. MC service server A requests the discreet listening function from MC service server B.

- MC user B places or receives an MCPTT or MCVideo private call to or from MC user C.

- MC service server A provides MC service client A with information concerning the initiation of the call, including the identity of MC user C, and also provides the media exchanged between the two parties in the call. MC service server B and MC service server A share the relevant information for this to take place.

- When the private call completes, the call completion is also conveyed to MC service client A.

NOTE 1: The scenario is the same whether MC user C, the other party in the private call, is receiving MC service from MC service server A or MC service server B.

NOTE 2: The scenario does not imply any requirement for media routing, whether MC user C receives service from MC service server A or MC service server B.

NOTE 3: The scenario also applies to emergency private calls.

## 4.3 Scenario 2: Discreet listening of MCPTT and MCVideo group calls

This scenario describes the case where authorized MC user A requests discreet listening for communications involving MC user B where MC service user B is within the authority of authorized MC user A, where MC user A and MC user B have the same primary MC service server, MC service server A. MC user B is a member of MC service group X together with MC users C to N, and therefore the communications in MC service group X are to be provided to MC user A. The primary MC service server of MC service group X is also MC service server A. The scenario is illustrated in figure 4.3.1-1 below.



Figure 4.3.1-1: Discreet listening of MCPTT or MCVideo group call

The scenario consists of the following aspects:

- Authorized MC user A identifies MC user B as the target for discreet listening, and the request for discreet listening is sent by MC service client A to MC service server A, which verifies that MC user A is authorized to perform discreet listening on MC user B. This aspect takes place before any communications involving MC user B can be subject to discreet listening.

- MC service server A identifies MC user B as a member of MC service group X

- A group member in MC service group X (one of MC users B or C to N) makes an MCPTT or MCVideo group call.

- MC service server A provides MC service client A with information concerning the initiation of the call, including the identity of the calling MC user, and also provides the media exchanged throughout the group call.

- When the group call completes, the call completion is also conveyed to MC service client A.

NOTE 1: The scenario does not determine whether authorized MC user A is a member of MC service group X or not.

NOTE 2: The scenario also applies to other variants of group call, such as emergency group call, imminent peril group call, broadcast group call and calls to temporary groups where MC user B is a group member.

NOTE 3: If any of MC users B or C to N is receiving MC service from a different MC service server from authorized MC user A, or if the group host MC service server is different from the MC service server serving authorized MC user A, the scenario is similar to that described in subclause 4.2.2 for private call with different MC service servers.

## 4.4 Scenario 3: Discreet listening of MCVideo pull

### 4.4.1 Scenario 3.1: Discreet listening of one to one MCVideo pull

This scenario describes the case where authorized MC user A requests discreet listening for MC user B where MC user B is within the authority of authorized MC user A, and authorized MC user A receives MCVideo pulls where MC user B is the initiator of the MCVideo pull request to a third MC user, or is the recipient of an MCVideo pull request from a third MC user and so provides video as a result of this request. As a one to one MCVideo pull is procedurally identical to an MCVideo private call, the scenarios are the same as those described within the present document in subclause 4.2.1 for MCVideo private call within a single MC service server, and in subclause 4.2.2 where the authorized MC user and target MC user are receiving service from different MC service servers.

### 4.4.2 Scenario 3.2: Discreet listening of one from server MCVideo pull

This scenario describes the case where authorized MC user A requests discreet listening for MC user B where MC user B is within the authority of authorized MC user A, and where authorized MC user A receives MCVideo pulls from the MCVideo server initiated by MC user B. In figure 4.4.2-1 below, MC user A and MC user B have the same primary MCVideo server, MCVideo server A.



Figure 4.4.2-1: Discreet listening of MCVideo pull from server

The scenario consists of the following aspects:

- Authorized MC user A identifies MC user B as the target for discreet listening, and the request for discreet listening is sent by MC service client A to MCVideo server A. This aspect takes place before any communications involving MC user B can be subject to discreet listening.

- MC user B initiates an MCVideo pull from the MCVideo server.

- MCVideo server A provides MC service client A with information concerning the initiation of the MCVideo pull, and provides the MCVideo media sent from the MCVideo server to MC user B.

NOTE 1: An alternative would be to notify authorized MC user A when MC user B requests to make an MCVideo pull, and allow MC user A to decide whether to receive the video media.

NOTE 2: Authorized MC user A may receive separate notifications when the MCVideo pull is initiated, and when the MCVideo is provided.

NOTE 3: The provision of MCVideo media to authorized MC user A may be in real time, or on demand with intermediate storage in the MCVideo server.

If MC user B receives MC service from a different MCVideo server, MCVideo server A will request the discreet listening function from the serving MCVideo server of MC user B.

## 4.5 Scenario 4: Discreet listening of MCVideo push

### 4.5.1 Scenario 4.1: Discreet listening of one to one MCVideo push

This scenario describes the case where authorized MC user A requests discreet listening for MC user B where MC user B is within the authority of authorized MC user A, and authorized MC user A receives MCVideo pushes initiated or received by MC user B. As a one to one MCVideo push is procedurally identical to an MCVideo private call, the scenarios are the same as those described within the present document in subclause 4.2.1 for MCVideo private call within a single MC service server, and in subclause 4.2.2 where the authorized MC user and target MC user are receiving service from different MC service servers.

### 4.5.2 Scenario 4.2: Discreet listening of one to server MCVideo push

This scenario describes the case where authorized MC user A requests discreet listening for MC user B where MC user B is within the authority of authorized MC user A, and where authorized MC user A receives MCVideo pushes to the MCVideo server that have been initiated by MC user B. In figure 4.5.2-1 below, MC user A and MC user B have the same primary MCVideo server, MCVideo server A.



Figure 4.5.2-1: Discreet listening of MCVideo push to server

The scenario consists of the following aspects:

- Authorized MC user A identifies MC user B as the target for discreet listening, and the request for discreet listening is sent by MC service client A to MCVideo server A. This aspect takes place before any communications involving MC user B can be subject to discreet listening.

- MC user B initiates an MCVideo push to the MCVideo server.

- MCVideo server A provides MC service client A with information concerning the initiation of the MCVideo push, and provides the MCVideo media sent from MC user B to the MCVideo server.

NOTE 1: An alternative would be to notify authorized MC user A when MC user B requests to make an MCVideo push, and allow MC user A to decide whether to receive the video media.

NOTE 2: Authorized MC user A may receive separate notifications when the MCVideo push is initiated, and when the MCVideo is provided.

NOTE 3: The provision of MCVideo media to authorized MC user A may be in real time, or on demand with intermediate storage in the MCVideo server. This aspect may need an additional requirement on media storage server.

If MC user B receives MC service from a different MCVideo server, MCVideo server A will request the discreet listening function from the serving MCVideo server of MC user B.

### 4.5.3 Scenario 4.3: Discreet listening of remotely initiated MCVideo push

This scenario describes the case where authorized MC user A requests discreet listening for communications involving MC user B where MC user B is within the authority of authorized MC user A, and where MC user C causes a remotely initiated MCVideo push from MC user B to MC user D. The scenario is illustrated in figure 4.5.3-1 below.



Figure 4.5.3-1: Discreet listening of remotely initiated MCVideo push

The scenario consists of the following aspects:

- Authorized MC user A identifies MC user B as the target for discreet listening, and the request for discreet listening is sent by MC service client A to MCVideo server A. This aspect takes place before any communications involving MC user B can be subject to discreet listening.

- MC user C initiates a remotely initiated MCVideo push procedure, wherein MC user B pushes video to MC user D.

- MCVideo server A provides MC service client A with information concerning the initiation of the MCVideo push including the identities of MC users C and D, and provides the MCVideo media sent from MC user B to MC user D.

NOTE 1: An alternative would be to notify authorized MC user A when MC user B initiates the MCVideo push, and to allow MC user A to decide whether to receive the video media.

NOTE 2: Authorized MC user A may receive separate notifications when the MCVideo pull is initiated, and when the MCVideo is provided.

NOTE 3: The provision of MCVideo media to authorized MC user A may be in real time, or on demand with intermediate storage in the MCVideo server. This aspect may need an additional requirement on media storage server.

NOTE 4: The scenario is the same where MC user C causes MC user D to push MCVideo media towards MC user B; MCVideo server A also sends the pushed video from MC user D to authorized MC user A.

If MC user B receives MC service from a different MCVideo server, MCVideo server A will request the discreet listening function from the serving MCVideo server of MC user B.

## 4.6 Scenario 5: Discreet listening of MCData SDS

This scenario describes the case where authorized MC user A requests discreet listening for communications involving MC user B where MC user B is within the authority of authorized MC user A, and where MC user A and MC user B have the same primary MCData server. The scenario is illustrated in figure 4.6.1-1 below.



Figure 4.6.1-1: Discreet listening of one to one MCData SDS

The scenario consists of the following aspects:

- Authorized MC user A identifies MC user B as the target for discreet listening, and the request for discreet listening is sent by MC service client A to MCData server A. This aspect takes place before any communications involving MC user B can be subject to discreet listening.

- MC user B sends or receives an MCData SDS data request to or from MC user C.

- MCData server A provides MC service client A with the MCData SDS data request, including relevant information such as conversation identifier and transaction identifier.

- If the recipient sends one or more disposition notifications, these are also sent to MC user A.

NOTE 1: The scenario applies whether the data is sent over the signalling plane or the media plane.

NOTE 2: The scenario applies whether the data is sent in standalone transactions, or as part of a session.

NOTE 3: The use applies to enhanced status sent over SDS.

NOTE 4: If authorized MC user A is receiving MC service from a different MCData server to that of MC user B, the serving MCData server of MC user A communicates with the serving MCData server of MC user B to provide the discreet listening service. This is similar to the case of MCPTT and MCVideo private calls described in subclause 4.2.2.

NOTE 5: If MC user B is sending or receiving SDS within a group, the scenario is similar to that described in subclause 4.3 for MCPTT and MCVideo group call.

## 4.7 Scenario 6: Discreet listening of MCData file distribution

### 4.7.1 Scenario 6.1: Discreet listening of file upload and file download

This scenario is similar to those for MCVideo push and MCVideo pull from server described in subclauses 4.4.2 and 4.5.2 of the present document.

### 4.7.2 Scenario 6.2: Discreet listening of one to one file distribution

This scenario describes the case where authorized MC user A requests discreet listening for communications involving MC user B where MC user B is within the authority of authorized MC user A, and where MC user A and MC user B have the same primary MCData server. The scenario is the same whether the file is distributed over HTTP or over the media plane. The scenario is illustrated in figure 4.7.2-1 below.



Figure 4.7.2-1: Discreet listening of one to one MCData file distribution

The scenario consists of the following aspects:

- Authorized MC user A identifies MC user B as the target for discreet listening, and the request for discreet listening is sent by MC service client A to MCData server A. This aspect takes place before any communications involving MC user B can be subject to discreet listening.

- MC user B sends or receives an MCData file distribution request to or from MC user C.

- MC service server A provides MC service client A with the transferred file, including relevant information such as the identity of MC user C, the conversation identifier and transaction identifier.

- The MCData download completed report is also sent to MC service client A.

NOTE 1: The scenario applies whether the file is sent over HTTP or the media plane.

NOTE 2: Authorized MC user A may receive separate notifications when the MCData file transfer is initiated, and when the MCData file is provided.

NOTE 3: The provision of the MCData file to authorized MC user A may be in real time, or on demand with intermediate storage in the MCData server.

NOTE 4: If authorized MC user A is receiving MC service on a different MCData server to that of MC user B, the serving MCData server of MC user A communicates with the serving MCData server of MC user B to provide the discreet listening service. This is similar to the case of MCPTT and MCVideo private calls described in subclause 4.2.2.

## 4.8 Scenario 7: Logging scenarios

### 4.8.1 General

According to the requirements for logging in 3GPP TS 22.280 [2] and 3GPP TS 22.281 [3] which are also reproduced in Annex A of the present document, mechanisms are to be provided to log both media and metadata for call related and call unrelated activity of the target MC service users and MC service groups.

The call related scenarios can be considered to be the same as those described in scenarios 1 to 6 related to discreet listening, except that the recipient of the information is a logging client or interface instead of the authorized user.

## 4.9 Scenario 8: Limitations on discreet listening due to regulatory constraints and operator security policies

### 4.9.1 Scenario 8.1: Private communication transmissions

This scenario describes the case where authorized MC user A requests discreet listening for communications involving MC user B where MC user B is within the authority of authorized MC user A. MC user C can be, but does not have to be within the authority of the authorized MC user A. The MC user C is not the target of the discreet listening request executed by the authorized MC user A. The scenario would allow MC user A to be part of the communication coming from MC user B, but not the communication coming from MC user C. The scenario is illustrated in figure 4.9.1-1 below.



Figure 4.9.1-1: Discreet listening with regulatory constraints on private communication transmissions

NOTE 1: As the communication originated from MC user C is restricted, authorized user A is not able to receive the full context of the communications from MC user B which may limit the usefulness of the discreet listening of user B.

NOTE 2: As authorized user A will know that user B and user C are communicating, and able to receive all conversation from user B, the security of user C is not preserved in this scenario.

### 4.9.2 Scenario 8.2: Group communication transmissions

This scenario describes the case where authorized MC user A requests discreet listening for a set of users being part of group communications involving MC user B to MC user D where MC user B to MC user D are within the authority of authorized MC user A. All other participants on these group communications can, but do not have to be within the authority of the authorized MC user A. The scenario would allow MC user A to be part of the communications coming from MC user B to MC user D, but not the communication coming from MC user E. The scenario is illustrated in figure 4.9.2-1 below.



Figure 4.9.2-1: Discreet listening with regulatory constraints on users being part of group communication transmissions

The scenario consists of the following aspect:

- Authorized MC user A is requesting group communication transmissions by identifying the target users being part of group communications.

NOTE 1: As the communication originated from MC user E is restricted, authorized user A is not able to receive the full context of the communications in the rest of the group which may limit the discreet listening service capability.

NOTE 2: As authorized user A will know that the other group members are communicating with user E, and able to receive all conversation from the rest of the group, the security of user E is not preserved in this scenario.

# 5 Key Issues

## 5.1 Key Issue 1: Selection of MC service for discreet listening

The single requirement for discreet listening [R-6.15.1-001] provided in 3GPP TS 23.280 [2] and reproduced in Annex A of the present document requires that all group or private communication transmissions from the target MC user are to be subject to discreet listening by an authorized MC user.

In practice, selection at the MC service level will automatically take place, as the MC service clients for each MC service will be used to place the discreet listening requests on behalf of the authorized MC user, for example if the authorized MC user only places the discreet listening request using an MCPTT client, only MCPTT transmissions will be available to the authorized MC user.

Within each of the MCPTT, MCVideo and MCData services, there are a number of separate services available and it is not clear whether the authorized MC user would wish to automatically receive content involving the target MC user within these separate services; for example whether the authorized MC user would require to receive MCData SDS transmissions but not MCData file upload and downloads.

NOTE: It is assumed that when discreet listening is invoked by the authorized MC user, the authorized MC user is provided with communications transmitted by the target MC user, and communications received by the target MC user.

Issues:

- Whether there should be granularity of discreet listening within each MC service, or whether all services within each MC service should always be provided to the authorized MC user following a request for discreet listening of a target MC user within an MC service.

## 5.2 Key issue 2: Group membership of authorized MC user for discreet listening

The target of discreet listening may be a member of an MC service group, and be able to take part in group communications. The authorized MC user will expect to receive all MC service group communication transmissions involving the target MC user, however the authorized MC user might not be defined as an MC service group member of the MC service group in which the target MC user is communicating.

Issues:

- Whether the authorized MC user should be a pre-defined member of an MC service group in order to receive group communications in which the target MC user is involved.

- Whether the authorized MC user should be temporarily made an MC service group member in order to receive group communications in which the target MC user is involved.

- Whether, if the authorized MC user is not an MC service group member, there should be any restriction on the communications involving the target MC user that are provided to the authorized MC user, e.g. provision of the target's transmissions to the MC service group, but not transmissions of other MC service group members.

- Whether any restrictions on requiring MC service group membership are different when the MC service group is defined in a different primary MC system to that of the authorized MC user.

- If the authorized MC user affiliates to the MC service group in order to receive the media in group communications, the affiliation of the authorized MC user to the MC service group may be visible to the target MC user and to other members of the MC service group; and the stage 1 requirement is that discreet listening takes place without the knowledge of the target MC user.

- How the authorized MC user is able to recover the content of communications within the group that are protected by end to end encryption.

Editor's note: Membership of a group homed in an interworked system is FFS.

## 5.3 Key issue 3: Discreet listening for MCVideo push and pull and MCData file upload and download

The MCVideo video push and video pull services each start with a negotiation phase, where information related to the video content to be pushed or pulled such as URL, media characteristics etc is provided and agreed. The MC user can be notified and asked to accept incoming video within a video push.

Similarly, the MCData file upload and file download services each start with a negotiation phase where information related to the file transfer such as URL is provided and agreed. The MC user can be notified and asked whether to accept an incoming file transfer.

The discreet listening service could either allow the authorized MC user who is the recipient of the information to accept video or data before that video or data is sent to the authorized MC user, or could be provided with the video or data sent to or from the target MC user of the discreet listening service automatically.

Issues:

- Whether the authorized MC user should be notified about the start of video push and pull or file upload or download transactions involving the MC user who is the target of discreet listening and given the choice to accept and receive the information or reject receiving the information; or whether the authorized MC user should always receive the information without any choice being needed.

- Whether the authorized MC user should receive notification both when the file upload or download negotiation phase takes place, and a second notification when the file upload or download takes place.

- Whether the authorized MC user should automatically be presented with the file date if a mandatory download takes place to the target MC user

- Whether the file content should be saved by the MCData server (or another suitable entity) until the authorized MC user decides to retrieve the file, and if so, whether there should be a time limit on this storage.

## 5.4 Key issue 4: Discreet listening of end to end encrypted calls

An authorized user may perform discreet listening on end to end encrypted communications, where those communications can be private calls, individual communications with a server (e.g. pull from or push to a server), and group calls where the target of the discreet listening is engaged in group communications. In order to comprehend the communications, the authorized user's MC service client needs to be provided with the end to end encryption key used to encrypt the content of the call.

NOTE: This key issue assumes that the decryption process is located in the authorized user's MC service client, to avoid violating the stage 1 requirement [R-5.12-009] in 3GPP TS 22.179 [2] for end to end encryption of media traffic.

For private or individual communications, a session key is used to encrypt the content of the communications, which is protected in transfer between the call participants by an encryption process making use of the identity of the destination party. The mechanism is described in 3GPP TS 33.180 [6].

For group communications, a GMK is originated by the GMS and protected in transfer to group members one at a time by an encryption process making use of the identity of each group member. The mechanism is described in 3GPP TS 33.180 [6].

According to the requirement in 3GPP TS 22.280 [2] and reproduced in Annex A of the present document, the participants in the call will not be aware of the discreet listening.

Issues:

- In order to successfully discreet listen to private or individual communications without violating the requirement for end to end encryption, the authorized user's MC service client needs access to the session key exchanged between the parties in the private or individual communication. To fulfil the requirement reproduced in Annex A.1, the parties in the call will not have knowledge of the authorized user possessing the encryption key.

- In order to successfully discreet listen to group communications without violating the requirement for end to end encryption, the authorized user's MC service client needs access to the GMK for the group. To fulfil the requirement reproduced in Annex A.1, the group members in the call will not have knowledge of the authorized user possessing the encryption key.

## 5.5 Key issue 5: Logging and replay of end to end encrypted calls

A logging entity requires to be able to record the content of end to end encrypted private calls, individual communications with a server (e.g. pull from or push to a server) and group calls. In order to permit replay of the content of the recorded calls, the encryption key must be available to provide decryption at some point in the process, either during recording, at some time during storage subsequent to recording, or on playback.

Issues:

- Whether the content should be decrypted at the point of recording, at some time during storage, or at the time of playback of the recorded material.

- How the entity performing the decryption obtains the encryption key to enable the decryption of the media content.

## 5.6 Key issue 6: Source MC service server for discreet listening of user in group call

An authorized user may perform discreet listening on an MC service user, where that MC service user is taking part in group communications. The primary MC service server of that MC service group may be a different MC service server to the primary MC service server of the target MC service user.

Issues:

- Which MC service server should provide the content of group call communications in which the target user takes part: the primary MC service server of the target user or the primary MC service server of the MC service group.

- How the solution prevents the discreet listening service being apparent to the target MC service user, or to other MC service group members.

## 5.7 Key issue 7: Discreet listening and logging for interconnected MC system

An authorized user may attempt to perform discreet listening on an MC service user that has a different primary MC system to that of the authorized user, where that target MC service user is taking part in private communications, or in group communications where the MC service group also has a different primary MC system to that of the authorized user. This could raise concerns about eavesdropping on communications in another security domain. The group case is illustrated in figure 5.7-1 below.



Figure 5.7-1: Discreet listening for a group entirely in a partner MC system

However, if MC service users in an MC system join an MC service group where that group has a different primary MC system which is connected by interconnection, it is likely that the MC system providing service for those MC service group members would wish to log communications within that group, and likely that an authorized user within that MC system may wish to perform discreet listening on group members who are receiving service in the same MC system as that authorized user. This is illustrated in figure 5.7-2 below.



Figure 5.7-2: Discreet listening or logging for group with group members in discreet listening /logging system

Issues:

- Discreet listening of individual or group communications may need to be restricted to target MC service users with the same primary MC system as the authorized user for discreet listening.

- Logging of individual or group communications may need to be restricted to target MC service users or groups which are receiving service in the same primary MC system as the logging entity.

- If discreet listening or logging of individual communications is permitted where the target is receiving service in an interconnected MC system, both the MC system where the target is receiving service and the MC system where the request for discreet listening or logging originates may need to authorize the discreet listening or logging service.

## 5.8 Key issue 8: Discreet listening and logging for migrated MC service user

An MC service user that has migrated to another MC system receives MC service within the security domain of that MC system.

Issues:

- The primary MC system of the MC service user and the migrated MC system of the MC service user may both wish to authorize discreet listening and/or logging of the migrated MC service user by the primary MC system of that migrated MC service user.

- The primary MC system of the migrated MC service users and the migrated MC system of the migrated MC service user may both wish to authorize any logging or discreet listening of the migrated MC service user by the migrated MC system.

- There may be a need to restrict the provided content of communications to that which is originated by the migrated MC service user, and not to provide content which originates from other users receiving service within the migrated MC system.

- There may be a need to restrict metadata relating to the communications to hide the identities and other information relating to MC service users and MC service groups whose primary MC system is the migrated MC system of the MC service user who is the target of the discreet listening or logging.

## 5.9 Key Issue 9: Discreet listening and logging for user receiving MC service on multiple devices

An MC service user may be service authorized on multiple MC service UEs, and may be receiving the same or different MC services on each of these. It is possible that an MC service user will receive the same communications content on more than one device simultaneously. Both the discreet listening and the logging services target a specific MC service user, and therefore both services will expect to obtain the content of communications and relevant communication related information whichever device the MC service user makes use of.

Issues:

- Whether there is any need to identify the MC service UE that was used for each communication, and how such identification of the relevant MC service UE is possible.

- Whether there is any need to capture or to remove duplicated content of the MC service user receives the same communications content on more than one MC service UE.

## 5.10 Key Issue 10: Logging of MC service users and MC service groups

An entity is required to perform logging of the communications and communications related information of MC service users and MC service groups.

Issues:

- Whether an existing functional entity such as an MC service client can provide the logging function, or whether a new functional entity is required.

- Whether new reference points are needed to support logging.

- Whether there are any explicit protocol transactions and procedures needed to support logging.

- The configuration needed to support logging.

- Whether the logging entity is considered a group member, and whether it requires affiliation to an MC service group, in order to log group communications.

- Whether any aspect of the replay equipment needed to replay recorded communications is in scope of standardization

## 5.11 Key Issue 11: Logging of MCData content server and message store services

An MCData user may make use of a content server for upload and download of MCData content. An MCData user may also have the use of a message store where content of MCData transactions can be stored for later retrieval. Logging of information stored on the content server or message store could be achieved by storage capabilities of those entities, or could be achieved using a separate MC logging function.

Issues:

- Whether logging of transactions to and from an MCData content server is required.

- Whether logging of transactions to and from a message store is required.

- Whether logging of transactions which involve a content server or a message store can be satisfied by the content server or message store providing logging as an intrinsic function without the need for separate MC logging function.

- If a separate MC logging function is required to log transactions to and from a message store or content server, which additional reference points are needed to fulfil the functionality.

## 5.12 Key Issue 12: Discreet listening of MCData content server and message store services

An MCData user may make use of a content server for upload and download of MCData content. An MCData user may also have the use of a message store where content of MCData transactions can be stored for later retrieval. An authorized user may require discreet listening of transactions between the MCData user and the the content server or message store. If provided, the authorized user may need access to the content of information exchanged, or may require notification that the information is being exchanged without needing the content.

Issues:

- Whether discreet listening of transactions to and from an MCData content server is required.

- Whether discreet listening of transactions to and from a message store is required.

- Whether discreet listening requires notification that transactions are taking place without providing the content, or whether the content itself is also needed.

- Whether the content of transactions needs to follow the same path as notification of the transactions, if both notification and content are required, or whether content can be accessible by the authorized user directly from the message store or content server.

- Whether activation of discreet listening against a target user also gives the authorized user access to previous transactions to or from the target user which have been stored in a content server or message store, or whether access is only possible to transactions in progress.

- Whether activation of discreet listening to a group gives access to transactions (e.g. for group SDS) which have been exchanged prior to that activation.

- Whether discreet listening allows the authorized user to receive synchronization between the message store client of an MCData user and a message store, for example when the MCData client uploads transactions that took place whilst operating in off-network mode.

- Whether discreet listening allows the authorized user access to data content which an MCData user has created and stored in a message store, without that content being sent to or received from another MCData user.

## 5.13 Key issue 13: Discreet listening towards an MC service group

The target of discreet listening can be an MC service group specified by the authorized user. The authorized user receives all the group communications of this target group in a real time manner.

The authorized user (listener) can be within the primary MC system of the target group, or can be in a partner MC system of the target group.

The following aspects need to be further studied to support group based discreet listening:

- Procedures and information flows based on the reuse of existing solutions;

- Configurations that are needed for the authorizations for discreet listening.

## 5.14 Key Issue 14: Limitations on discreet listening due to regulatory constraints and operator security policies

An authorized MC user has requested discreet listening either on one MC user or a group of MC users. Regulatory constraints and operator security policies can require specifying the exact communication transmissions that are allowed to be part of the discreet listening service, which would result in limitations on discreet listening on all parties in the communication. The communication transmissions from a single target user as well as target users within a group can listened to by the authorized user while leaving everything else out of scope of the requested discreet listening. The regulatory constraints and operator security policies can have impact on all types of communication transmissions and is therefore mission critical service independent.

Issues:

- How only the communication transmissions coming from the target MC user involved in a private communication can be part of discreet listening.

- How only the communication transmissions coming from one target MC user or a group of target MC users involved in a group communication can be part of discreet listening.

- How any other communication transmissions are made unavailable to the authorized MC user, as they are not part of discreet listening requests.

- Whether any of the communication related signalling should be restricted.

NOTE: There may be security issues relating to the users that are outside the scope of the discreet listening, as the fact that communications are taking place, and the contents of those communications sent to those users is available to the authorized user.

# 6 Solutions

## 6.1 Solution 1: Functionality for discreet listening

### 6.1.1 Description

#### 6.1.1.1 Functional model

Discreet listening is carried out by an authorized user, who requests discreet listening for the communications of another user. The authorized user will require a client entity capable of fulfilling the discreet listening request. The functionality required is the same as that of an MC service client, with the addition of the capability to request discreet listening and specify a target MC service user. Therefore the solution is to reuse the MC service client, and make no additions to the functional model.

This solution addresses aspects of key issue 1, Selection of MC service for discreet listening, and key issue 2, Group membership of authorized user for discreet listening.

#### 6.1.1.2 Configuration

The user profiles for MCPTT, MCVideo and MCData which are specified in 3GPP TS 23.379 [7], 3GPP TS 23.281 [8] and 3GPP TS 23.282 [9] will need additional configuration to be added as shown in Table 6.1.1.2-1 below.

Table 6.1.1.2-1: Addition to MC service user profiles (on network)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Reference | Parameter description | MCPTT UE | MCPTT Server | Configuration management server | MCPTT user database |
|  | Authorized to perform discreet listening on another MC service user | Y | Y | Y | Y |
|  | List of users upon whom discreet listening can be invoked |  |  |  |  |
|  | > MC service ID | Y | Y | Y | Y |

In Table 6.1.1.2-1 'MC service' represents one of MCPTT, MCVideo or MCData.

#### 6.1.1.3 Procedures

##### 6.1.1.3.1 General

New procedures are added to allow the MC service client of the authorized user to invoke and revoke discreet listening of a target MC user, and to allow the MC service server to provide the content of calls in which the target user is involved.

##### 6.1.1.3.2 Discreet listening invocation and revocation procedures

The procedure allows the MC service client of the authorized user to request discreet listening of a target MC service user. The procedure is illustrated in figure 6.1.1.3.2-1 below.



Figure 6.1.1.3.2-1: Discreet listening invocation

The information flows needed to support such a procedure are shown in tables 6.1.1.3.2-1 and 6.1.1.3.2-2 below.

Table 6.1.1.3.2-1: Discreet listening activation request

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MC service ID | M | MC service ID of the target of the discreet listening request |

Table 6.1.1.3.2-2: Discreet listening activation response

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MC service ID | M | MC service ID of the target of the discreet listening request |
| Result | M | Indicates the success or failure of the discreet listening request |

Invocation of discreet listening of a target MC service user will result in all communications sent or received to any MC service client on which the target MC service user is receiving MC service being provided to the authorized user.

A similar procedure, not illustrated here, is required for revocation of the discreet listening function.

##### 6.1.1.3.3 Provision of discreet listening content for private communications

When the target user makes or receives a private call or initiates individual communications with a server, the authorized user needs to be informed and provided with the media. Figure 6.1.1.3.3-1 below illustrates a procedure where discreet listening target MC service client 1 sets up a call.



Figure 6.1.1.3.3-1: Discreet listening of target initiated private call

The procedure is similar if the target of the discreet listening is the recipient of the private call.

If the target initiated the private call, the discreet listening call request may include the client ID associated with the MC service client on which the target initiates the call. If the target receives a request for a private call, the discreet listening call request may include the client ID(s) of the MC service clients on which the private call request is received.

NOTE: If the MC service server does not receive the 'discreet listening call response' for any reason, the call should still proceed so that the requirement that the call is not affected and the target user is not aware of the discreet listening process is satisfied.

##### 6.1.1.3.4 Provision of discreet listening content for group communications

When the target user makes or receives a group call, the authorized user needs to be informed and provided with the media. Figure 6.1.1.3.4-1 below illustrates a procedure where discreet listening target MC service client 2 is a receiving party in a group call initiated by another affiliated group member.



Figure 6.1.1.3.4-1: Discreet listening of target initiated group call

If the target initiated the group call, the discreet listening call request may include the client ID associated with the MC service client on which the target initiates the call. If the target receives a request for a group call, the discreet listening call request may include the client ID(s) of the MC service clients on which the group call request is received.

The procedure is similar if the target of the discreet listening is the initiator of the group call.

NOTE 1: If the MC service server does not receive the 'discreet listening call response' for any reason, the call should still proceed so that the requirement that the call is not affected and the target user is not aware of the discreet listening process is satisfied.

NOTE 2: It is irrelevant whether the authorized user is or is not a member of the MC service group.

##### 6.1.1.3.5 Information flows for discreet listening

A single pair of information flows can support provision of discreet listening content of individual communications and group communications. Suitable information elements are shown in tables 6.1.1.3.5-1 and 6.1.1.3.5-2 below.

Table 6.1.1.3.5-1: Discreet listening call request

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MC service ID | M | MC service ID of the target of discreet listening |
| MC service client ID list  (see NOTE) | O | List of MC service client IDs of the target user on which the call is requested |
| MC service ID | M | MC service ID of the other party in individual call, or MC service ID of talking party in group call |
| Call direction | M | Indicates whether the target or another party initiated the call |
| Call type | M | Indicates the type of communication (private call, group call etc) |
| MC service group ID | O | Provided if the communication is a group call |
| NOTE: MC service client ID identifies a specific installation of an MC service client on an MC service UE and is provided to the MC service server at service authorization of the MC service user. It may be equivalent to the client IDs specified in 3GPP TS 24.379 [10], 3GPP TS 24.281 [11] and 3GPP TS 24.282 [12]. | | |

Table 6.1.1.3.5-2: Discreet listening call response

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MC service ID | M | MC service ID of the target of discreet listening |
| Result | M | Indicates the success or failure of the discreet listening call request |

### 6.1.2 Impacts on existing nodes and functionality

This solution results in the following impacts on existing entities and reference points:

- MC service clients and MC service-1 reference points: addition of functionality to request discreet listening and to specify a target MC user.

- MC service user configuration: authorization to request discreet listening on a list of target MC service IDs.

- A new procedure to request discreet listening specifying a target MC service user.

- A new procedure to provide the content of discreet listening.

In each case, MC service is one of MCPTT, MCVideo or MCData.

### 6.1.3 Solution Evaluation

This solution allows discreet listening to be achieved with minimal changes to the functional model as it only requires enhancement to existing functional entities and reference points. It also allows discreet listening to be invoked on a service dependent basis as it is achieved as a function of the MC service specific MC service clients. It supports the situations where the MC service user is receiving MC service on multiple MC service clients.

## 6.2 Solution 2: Discreet listening of MCVideo push and pull

### 6.2.1 Description

#### 6.2.1.1 Overview

This solution addresses the MCVideo aspects of key issue 3 for discreet listening of MCVideo push and pull.

#### 6.2.1.2 Invocation

Discreet listening is activated by the MC service client of the authorized user according to the invocation procedures described in subclause 6.1.1.3.2 of the present document.

#### 6.2.1.3 MCVideo push discreet listening procedure

The procedure for discreet listening of a one to server push is shown in figure 6.2.1.3-1 below.



Figure 6.2.1.3-1: MCVideo push to server discreet listening

Steps 1 to 7 are described in 3GPP TS 23.281 [3] subclause 7.4.2.4, the procedure for one to server video push. Additional steps to support discreet listening are as follow:

11. The MCVideo server notifies MCVideo client 2 of the authorized user that MCVideo client 1 has been authorized to push video to the MCVideo server. The notification includes the MCVideo ID of the MCVideo user and may include an MCVideo client ID of the MCVideo client from which the request to push video to the server was made. This step may take place at any time following step 2.

12. The authorized user is notified and decides whether to receive the MCVideo stream, or whether to just remain aware that an MCVideo push is taking place from the target MCVideo user of MCVideo client 1.

13. MCVideo client 2 provides the response to the MCVideo server, indicating whether the authorized user wishes to receive the video stream or not.

NOTE: Steps 12 and 13 may utilise an automatic process, such that a human user does not need to make a decision at the time that the video stream push commences.

If the authorized user decides to receive the video stream, steps 14 and 15 establish the media plane and transmission control, and transmit the video to the authorized user. Steps 16 and 17 complete the transaction.

If step 14 is completed before step 5 occurs, i.e. the media plane is set up to the authorized user but video streaming has not commenced from MCVideo client 1, the video stream sent to MCVideo client 2 of the authorized user in step 15 does not start until the stream in step 5 is received by the MCVideo server.

If step 14 has not completed before step 5 occurs, i.e. the MCVideo stream from MCVideo client 1 has commenced before the media plane is setup between the MCVideo server and MCVideo client 2 of the authorized user, the video stream in step 15 is either delayed so that the authorized user is able to view the stream from its commencement, or the stream is not delayed and so the authorized user receives the stream in real time, but does not receive the start of the video stream.

Editor's note: It is FFS whether the decision to delay or to truncate the start of the video stream sent to the authorized user is determined by configuration or by some other mechanism.

The same procedure can be followed between the MCVideo server and MCVideo client 2 of the authorized user where the MCVideo push is remotely initiated as described in subclause 7.4.2.5 of 3GPP TS 23.281 [3], and where the MCVideo push is sent to a group as described in subclause 7.4.2.6 of 3GPP TS 23.281 [3].

#### 6.2.1.4 MCVideo pull discreet listening procedure

The procedure for discreet listening of a one from server pull is shown in figure 6.2.1.4-1 below.



Figure 6.2.1.4-1: MCVideo pull from server discreet listening

Steps 1 to 7 are described in 3GPP TS 23.281 [3] subclause 7.3.2.4, the procedure for one from server video pull. Additional steps to support discreet listening are as follow:

11. The MCVideo server notifies MCVideo client 2 of the authorized user that MCVideo client 1 has been authorized to pull video from the MCVideo server. The notification includes the MCVideo ID of the MCVideo user and may include an MCVideo client ID of the MCVideo client from which the request to pull video from the server was made. This step may take place at any time following step 2.

12. The authorized user is notified and decides whether to receive the MCVideo stream, or whether to just remain aware that an MCVideo pull is taking place to the target MCVideo user of MCVideo client 1.

13. MCVideo client 2 provides the response to the MCVideo server, indicating whether the authorized user wishes to receive the video stream or not.

NOTE: Steps 12 and 13 may utilise an automatic process, such that a human user does not need to make a decision at the time that the video stream pull commences.

If the authorized user decides to receive the video stream, steps 14 and 15 establish the media plane and transmission control, and transmit the video to the authorized user. Steps 16 and 17 complete the transaction.

If step 14 is completed before step 5 occurs, i.e. the media plane is set up to the authorized user but video streaming has not commenced from the MCVideo server, the video stream sent to MCVideo client 2 of the authorized user in step 15 does not start until the stream in step 5 starts streaming from the MCVideo server.

If step 14 has not completed before step 5 occurs, i.e. the MCVideo stream from the MCVideo server has commenced before the media plane is setup between the MCVideo server and MCVideo client 2 of the authorized user, the video stream in step 15 is either delayed so that the authorized user is able to view the stream from its commencement, or the stream is not delayed and so the authorized user receives the stream in real time, but does not receive the start of the video stream.

Editor's note: It is FFS whether the decision to delay or to truncate the start of the video stream sent to the authorized user is determined by configuration or by some other mechanism.

#### 6.2.1.5 Information flows for discreet listening of MCVideo push and pull

A single pair of information flows can support the request and response for discreet listening of MCVideo push and pull video transfers. Suitable information elements are shown in tables 6.2.1.5-1 and 6.2.1.5-2 below.

Table 6.2.1.5-1: MCVideo push-pull discreet listening request

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MCVideo ID | M | MCVideo ID of the target of discreet listening |
| MCVideo client ID (see NOTE) | O | MCVideo client ID of the MCVideo client on which the target user is requesting to push or pull video |
| MCVideo ID | O | MCVideo ID of third party requesting remote MCVideo push, if applicable |
| Push/pull | M | Indicates whether the video is being pushed to or pulled from the target MCVideo client |
| MC service group ID | O | Provided if the communication is a push to an MCVideo push |
| NOTE: MCVideo client ID identifies a specific installation of an MCVideo client on an MCVideo UE and is provided to the MCVideo server at service authorization of the MCVideo user. It may be equivalent to the client ID specified in 3GPP TS 24.281 [11]. | | |

Table 6.2.1.5-2: MCVideo push-pull discreet listening response

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MCVideo ID | M | MCVideo ID of the target of discreet listening |
| Video stream reception | M | Indicates whether the authorized user wishes to receive the video stream |

The information elements for MCVideo push-pull discreet listening complete request and response are derived from those employed in steps 6 and 7 of the MCVideo push and pull procedures described in 3GPP TS 23.281 [3], and are illustrated in tables 6.2.1.5-3 and 6.2.1.5-4 below.

Table 6.2.1.5-3: MCVideo push-pull discreet listening complete request

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MCVideo ID | M | MCVideo ID of the target of discreet listening |
| Cause | M | End of communication cause |

Table 6.2.1.5-4: MCVideo push-pull discreet listening complete response

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MC service ID | M | MC service ID of the target of discreet listening |

### 6.2.2 Impacts on existing nodes and functionality

This solution results in the following impacts on existing entities and reference points:

- MCVideo clients and MCVideo-1 reference points: addition of functionality to offer and accept discreet listening MCVideo push and pull content.

- New procedures to provide discreet listening of MCVideo push and pull transactions.

- New configuration parameters may be needed to determine whether the MCVideo server truncates or caches video streams forwarded to the authorized user.

- New configuration parameters may be needed to authorize the discreet listening of MCVideo push and pull transactions.

### 6.2.3 Solution Evaluation

This solution allows discreet listening of MCVideo push and pull transactions to be achieved with minimal changes to existing MCVideo functionality, as the provision of discreet listening is based on existing MCVideo push and pull procedures. The solution includes a means of identifying the MCVideo client where an MCVideo user is receiving MCVideo service from multiple MCVideo clients. Additional configuration parameters are likely to be needed to support the service.

## 6.3 Solution 3: Functionality for on-network logging and replay

### 6.3.1 Description

#### 6.3.1.1 Functional model

To support on-network logging and replay, existing common service core functional entities are reused. The MC logging function makes use of a new MC logging client which has a subset of the functionality of an existing MC service client, in that it can receive communications information and communications content relating to logged users, but cannot set up calls or demand to take part in calls. Provision of call related information and call content is achieved by configuration in the MC service server. The MC logging client uses an MC service ID to allow call related information and call content to be routed to the MC logging client, reusing functionality from existing reference points.

NOTE 1: An MC logging function may contain multiple MC service clients to allow the separate services MCPTT, MCVideo and MCData to be logged within the same function. However this is out of scope of the description of the functional model.

Figure 6.3.1.1-1 below illustrates the functional entities and reference points of the common services core in the application plane that are used for logging.



Figure 6.3.1.1-1: Common services core functional model for logging

In Figure 6.3.1.1-1, the MC logging function is configured with the list of MC service IDs and MC service groups that the logging function will log using reference point CSC-4. The group management client receives configuration for groups that are to be logged. The identity management client allows the logging function to be authorized for logging service using reference point CSC-1, using either security credentials supplied by a user or supplied by the logging application. The key management client obtains keys using reference point CSC-8 to protect signalling information between MC service server and MC service client. Keys may be obtained to protect media if the solution is intended to log communications with any end to end encryption removed.

NOTE 2: The means of protecting media and communications related information during storage within the MC logging function is outside the scope of this solution.

The MC replay function receives the necessary security information needed to replay logged communications by CSC-8. A user of the replay function, or an automatic function of the replay function, will perform the necessary authorizations to retrieve logged communications, and CSC-1 will be used to verify the authenticity and authorization of the user or function.

NOTE 3: Inclusion of the mechanisms for MC service user authentication and authorization for use by the replay function within this solution allows the user organization to require the same security processes to access logged information as the security processes that are used to communicate within the MC service. Alternative solutions are possible, but not considered within this solution.

The MC logging function and MC replay function are in the same security domain as the MC system for which communications are logged.

The interface MCLog-10 between the logging recorder and the replay client to retrieve communications is out of scope of this solution. MCLog-10 does not need to use 3GPP access for connectivity. Information relating to the user of the logging replay function and any profile for this replay function user are out of scope of this solution.

Figure 6.3.1.1-2 below shows the MC service related application plane entities used to log communications.



Figure 6.3.1.1-2: MC service related application plane functional model for logging

In figure 6.3.1.1-2, the MC logging function may comprise MC logging clients dedicated to MCPTT, MCVideo and MCData. Each MC logging client is identified by a service specific identity, namely the MCPTT ID, MCVideo ID or MCData ID of the client. Call related information concerning the targets of logging are sent to the MC logging function via MClog-1, which is based on the MCservice-1 reference points (i.e. MCPTT-1, MCVideo-1 etc) but does not permit calls to be initiated by the MC logging function. Media plane communications content is provided to the media reception function of the MC logging client via MCLog-2, which is based on unicast media distribution reference points MC service-7 (i.e. MCPTT-7, MCVideo-7 etc), and floor control or media control information provided during calls is provided via MCLog-3.

Editor's note: MCData services may require further functionality to be described.

#### 6.3.1.2 Configuration

The MC logging equipment will require configuration to determine which MC service users and which MC servive groups are required by that MC logging equipment. Table 6.3.1.2-1 below illustrates the identity specific configuration data applicable to each MC logging equipment. It is expected that the MC logging equipment configuration will not be added into existing MC service user configuration tables, but will have a unique configuration table.

Editor's note: It is expected that further configuration information will be needed. This table is intended to contain initial information only.

Table 6.3.1.2-1: MC logging equipment configuration

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Reference | Parameter description | MC logging equipment | MC service server | Configuration management server |
|  | MC service identity of MC logging client | Y | Y | Y |
|  | List of users to be logged |  |  |  |
|  | > MC service ID | Y | Y | Y |
|  | List of groups to be logged |  |  |  |
|  | > MC service group ID | Y | Y | Y |

The need to log MC service group calls will require MC service group configuration information to include the list of MC logging equipments. The additions shown in table 6.3.1.2-2 will be made to table A.4-2 (MC service group configuration) in 3GPP TS 23.280 [2].

Editor's note: Further configuration information related to logging may be added in addition to the identities listed in table 6.3.1.2-2 below.

Table 6.3.1.2-2: Addition to common group configuration data (on network) for logging

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Reference | Parameter description | MC service UE | MC service Server | Group management server |
|  | List of logging equipments that log MCPTT calls |  |  |  |
|  | >MCPTT ID |  | Y | Y |
|  | List of logging equipments that log MCVideo calls |  |  |  |
|  | >MCVideo ID |  | Y | Y |
|  | List of logging equipments that log MCData calls |  |  |  |
|  | >MCData ID |  | Y | Y |

Additionally, the MC service ID for the logging equipment that is assigned to log the communications of each MC service user will need to be added to the user profiles for MCPTT in 3GPP TS 23.379 [7], for MCVideo in 3GPP TS 23.281 [8] and for MCData in 3GPP TS 23.282 [9].

#### 6.3.1.3 Procedures

To initialise the logging function, the MC logging equipment will perform service authorization to each of the MC service servers following the procedure for authentication and authorization the primary MC system specified in 3GPP TS 23.280 [2] subclause 10.6.1.

It is not envisaged that any explicit protocol exchange will be carried out in order to start logging communications of identified MC service users and MC service group. Once service authorized, the MC logging equipment will be implicitly affiliated to all its configured MC service groups. However a procedure may be needed to show the interaction between the service authorization of the logging equipment and the implicit authentication of the MC logging client of the MC logging equipment to the logged MC service groups.

Procedures will need to be defined to illustrate the provision of communications content and communications related information to the MC logging equipment. The functionality of the reference points MCLog-1, MCLog-2 and MCLog-3 that provide this information will need to be defined, derived from existing reference points.

The MC service server will send the MC logging equipment:

- Notification of service authorization for each logged MC service user.

- Notification of MC service group affiliations of each member of each logged MC service group, and notifications of group affiliations from each logged MC service user.

- Notifications of call set up information for each logged MC service user and MC service group

- Notifications of floor control, transmission control and media control information for each MC service user and MC service group

- The content of each media exchange to and from each logged MC service user and within each logged MC service group

- Notifications of end of logged calls

Each notification will include a timestamp.

Each notification will include the identity of the MC service user being logged, and may include an MC service client ID or list of MC service client IDs of the MC service client(s) on which the MC service user is sending or receiving media. Where group calls are logged, the MC service ID of the transmitting party is included in the notification, and an MC service client ID relating to the MC service client from which the transmission is being made may also be included.

NOTE: The MC service client ID identifies a specific installation of an MC service client on an MC service UE and is provided to the MC service server at service authorization of the MC service user. It may be equivalent to the client IDs specified in 3GPP TS 24.379 [10], 3GPP TS 24.281 [11] and 3GPP TS 24.282 [12].

The MC replay equipment will require authorization of the MC service user making use of the MC replay equipment, following the procedure for authentication and authorization the primary MC system specified in 3GPP TS 23.280 [2] subclause 10.6.1. Configuration and authorization of the user of the MC replay equipment is out of scope of this solution.

Editor's note: It is FFS whether authorization to use MC replay equipment is within the scope of the user profile of an MC service user as defined in the MC service specifications.

### 6.3.2 Impacts on existing nodes and functionality

New entities are introduced in this solution, specifically the MC logging equipment and its constituent MC logging client together with MC logging storage and the MC replay equipment containing the MC replay client. The new MC logging client is based on existing MC service clients to maximise reuse of existing functionality and reference points.

The process for authentication and service authorization use existing functional entities, reference points and procedures.

New configuration will be introduced to configure logging equipment, and to configure MC service groups with the list of MC logging equipments that will log MC service group communications.

New procedures for logging call related information and call contents will be required. However these can be based on existing procedures for call setup and floor, transmission and media control within calls.

Interactions between MC logging client, logging storage and the MC replay client are not specified within this solution and so have no impact on existing nodes and functionality.

### 6.3.3 Solution Evaluation

This solution defines new functional entities and reference points to fulfil the on-network logging requirement together with reuse of existing common services core functional entities and reference points. The new functional entities and reference points will be based on the functionality of existing MC service clients and associated reference points. The solution includes a means of identifying the MC service client where an MC service user is receiving MC service from multiple MC service clients.

A set of procedures will need to be defined to show the invocation of logging functions on logged calls.

## 6.4 Solution 4: On-network logging for interconnection and migration

### 6.4.1 Description

#### 6.4.1.1 General

This solution builds on solution 3, 'Functionality for on-network logging and replay' to add the case where the logging equipment receives service from its primary MC system, but the target of logging is receiving service in a partner MC system. The target of logging may be receiving MC service in its primary MC system, or may have migrated to that MC system from another MC system.

#### 6.4.1.2 Functional model

The functional model in solution 3 is expanded to show the interconnection to a different MC system. This is shown in figure 6.4.1.2-1 below.



Figure 6.4.1.2-1: Common services core functional model for logging with interconnection

In Figure 6.4.1.2-1, the interaction between the MC logging equipment and the MC replay equipment is not shown and remains according to solution 3.

The configuration management server in the primary MC system of the MC logging equipment provides the MC logging equipment with the list of MC service users and MC service groups that the MC logging equipment logs. This can include users and groups that receive service in partner MC systems. The list of users and groups receiving service in the partner MC system is shared by the configuration management server in the primary MC system of the MC logging equipment with the configuration management server in the partner MC system using reference point CSC-17, and authorized users or administrators of the partner MC system can locally modify or authorize the list. When this configuration in the partner MC system is provided to the partner MC service server, the partner MC service server can determine which calls should be provided to the primary MC system of the MC logging equipment to allow logging to take place.

There needs to be interaction between the group management servers in the two MC systems using reference point CSC-16 so that the group management server in the partner MC system can authorize the MC logging equipment to be a member of MC service groups which are hosted in that partner MC system.

Figure 6.4.1.2-2 below shows the MC service related application plane entities used to log communications originating from a partner MC system.



Figure 6.4.1.2-2: MC service related application plane functional model for logging for interconnection

In figure 6.4.1.2-2, an additional reference point MCLog-4 is added between MC service servers compared with the functional model in solution 3. MCLog-4 carries call related information and call content from the partner MC service server to the primary MC service server, and is based on reference point MCX-1. Compared with MCX-1, MCLog-4 only permits communications information to originate from the partner MC service server and to flow via the primary MC service server to the MC logging equipment, and does not permit calls to be set up in the opposite direction.

#### 6.4.1.3 Configuration

##### 6.4.1.3.1 General

The MC logging equipment configuration outlined in solution 3 remains unchanged for interconnection and migration. The list of users and groups to be logged can include users and groups receiving service in a partner MC system of the MC logging equipment.

The impact of logging for MC service groups, and a configuration for logging of group communications where the group host is a partner MC system of the MC logging equipment is presented in subclause 6.4.1.3.2.

The impact of logging for MC service users is presented as three alternative solutions for logging of individual communications in a partner MC system, contained in subclauses 6.4.1.3.3, 6.4.1.3.4 and 6.4.1.3.5. Individual communications include private calls between MC service users and communications between an MC service user and a server. It is necessary for a primary MC system to be provided with the MC service IDs of the MC logging clients of logging equipments which are providing logging service in a partner MC system, and for authorized users or administrators of the primary MC system to be able to authorize this logging from a partner MC system. The three options in the three subclauses provide this information in alternative ways.

##### 6.4.1.3.2 Logging of group communications in partner system

No changes are needed to group configuration information. The common group configuration (on-network) includes the MC service IDs of the MC logging clients of the MC logging equipment which is providing the logging service in a partner MC system of the group.

##### 6.4.1.3.3 Logging of individual communications – option 1

In solution 3, the list of MC service IDs to be logged by an MC logging equipment are listed in the configuration of the MC logging equipment, and the MC service IDs relating to the MC logging equipment are not listed in the user profiles of the target MC service users. In the solution described in the present subclause, the user profiles of MC service users are expanded to include the MC service IDs of the responsible MC logging equipment. Thus an on-network MC service user profile will gain the configuration paremeters listed in table 6.4.1.3.3-1.

Table 6.4.1.3.3-1: Addition to MC service user profile for logging of individual communications

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Reference | Parameter description | MCPTT UE | MCPTT server | Configuration management server | MCPTT user database |
|  | List of MC logging clients which log communications of the MC service user |  |  |  |  |
|  | > MC service ID | N | Y | Y | Y |

In Table 6.4.1.3.3-1 'MC service' represents one of MCPTT, MCVideo or MCData.

To support interconnection, the MC service IDs of the MC logging clients will include those contained in MC logging equipment that is providing logging service in a partner MC system. In the case of migration, the partner MC system of the migrated MC service user will receive a user profile from the primary MC system of the MC service user which includes the list of MC logging equipment in the primary MC system of the MC service user (and in any other MC systems) which log the communications of that MC service user.

NOTE: This solution has similarities with the configuration for MC service groups, where the group members are listed in the group configuration information, and the list of groups for each MC service user is listed in the user profile.

##### 6.4.1.3.4 Logging of individual communications – option 2

In this solution, the configuration table of the MC logging equipment and its target MC service users described in solution 3, table 6.3.1.2-1, is provided to the partner MC system. The partner MC system therefore may receive multiple configuration tables from the primary MC system of the MC logging equipment where each configuration table identifies an MC logging equipment and the list of MC service users to be logged. The configuration information will need to be analysed in the partner MC system to determine which MC service servers need to be provided with the information to permit logging based on the list of target MC service users.

NOTE: The primary MC system of the MC logging equipment may provide the partner MC system with a configuration table relevant to each MC logging equipment where only target MC service users that may receive MC service in the partner MC system are listed (instead of the full set of users that the MC logging equipment logs).

##### 6.4.1.3.5 Logging of individual communications – option 3

In this solution, a single configuration table is provided to the partner MC system that lists the MC service identities of the MC logging equipments which provide logging service in their primary MC system and their set of logged MC service users. Such a configuration table is shown in table 6.4.1.3.5-1.

Table 6.4.1.3.5-1: MC logging equipment configuration for provision to partner MC system

|  |  |  |  |
| --- | --- | --- | --- |
| Reference | Parameter description | MC service server | Configuration management server |
|  | MC service identity of MC logging client |  |  |
|  | > MC service ID | Y | Y |
|  | > List of users to be logged |  |  |
|  | >> MC service ID | Y | Y |

The configuration information will need to be analysed in the partner MC system to determine which MC service servers need to be provided with the information to permit logging based on the list of target MC service users.

NOTE 1: The primary MC system of the MC logging equipment may provide the partner MC system with a configuration table relevant to each MC logging equipment where only target MC service users that may receive MC service in the partner MC system are listed (instead of the full set of users that the MC logging equipment logs).

NOTE 2: The table could also include a list of MC service groups to be logged for each MC logging equipment.

#### 6.4.1.4 Procedures

Solution 3 discusses the need to add procedures to the MC service specifications to illustrate the inclusion of the MC logging equipment in communications. In the case of interconnection, the generic procedures for interconnection described in 3GPP TS 23.280 [2] subclause 10.14 also apply to procedures for logging, allowing the relevant partner MC system to be determined and authorization for the logging to take place by both the primary and partner MC systems.

### 6.4.2 Impacts on existing nodes and functionality

An additional reference point is added to the MC service servers, MCLog-4, to allow communication related information and communication content to be passed from the MC service server where the communications are hosted to the primary MC service server of the MC logging equipment. However this is based on existing reference point MCX-1, and can be considered a reduced function set of MCX-1.

Additional configuration is added beyond that specified in solution 3, to allow MC logging equipment providing logging in one MC system to receive the communications for logging from a partner MC system.

### 6.4.3 Solution Evaluation

This solution expands the solution defined in solution 3 to allow logging where the logging equipment is providing logging services in a different MC system to that of the MC logging equipment.

Three options are provided to provide configuration to a partner MC system to enable logging of individual communications. Of these, option 1 which adds the MC service ID associated with the MC logging equipment to the user profile is preferred as it does not add further configuration tables to be exchanged between primary and partner MC systems to enable interconnection and migration, and does not require any analysis in the partner MC system to determine which MC service servers need to be provided with the information.

## 6.5 Solution 5: Discreet listening for interconnection and migration

### 6.5.1 Description

#### 6.5.1.1 Functional model

Solution 1 proposes that discreet listening within a single MC system is a functionality available to an authorized user, and therefore no changes are needed to the functional models for MC services. This will also be the case for interconnection and migration.

#### 6.5.1.2 Configuration

##### 6.5.1.2.1 General

The additional authorization to perform discreet listening to the user profiles for MCPTT, MCVideo and MCData which is proposed in solution 1 includes lists of users upon whom discreet listening can be invoked: these can include users that receive service in partner MC systems and therefore no further configuration is needed for interconnection and migration for the authorized user.

However, an MC system that provides MC service to a target for discreet listening will need to authorize requests for discreet listening that originate from a partner MC system. Three options are provided in the following subclauses as means to provide configuration to another MC system to allow such authorization to take place.

##### 6.5.1.2.2 User profile authorization of discreet listening – option 1

To permit discreet listening from a partner MC system, in this option the user profile of the target for discreet listening is modified to include the list of authorized users that are able to perform discreet listening on that target user. This will entail additions to the user profiles for MC service users as shown in table 6.5.1.2.2-1 below.

Table 6.5.1.2.2-1: Addition to MC service user profiles (on network)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Reference | Parameter description | MC serviceUE | MC service Server | Configuration management server | MC service user database |
|  | List of authorized users who can perform discreet listening on this MC service user |  |  |  |  |
|  | > MC service ID | N | Y | Y | Y |

In Table 6.5.1.2.2-1 'MC service' represents one of MCPTT, MCVideo or MCData.

Therefore, if an authorized user in a partner MC system of an MC service user is authorized to perform discreet listening on that MC service user, that authorized user's MC service identity will be configured in the user profile of the target MC service user. When an MC service user migrates to a partner MC system, the user profile for migration provided to the partner MC system of that MC service user will list authorized users permitted to perform discreet listenting on that MC service user, including those authorized users who receive MC service in the primary MC system of the migrating MC service user, or in any other MC system. The inclusion of this information in the user profile allows the MC service server in the partner MC system which provides service to the target MC service user to authorize requests for discreet listening when they arise.

##### 6.5.1.2.3 Sharing the user profile for authorized users – option 2

In this option, the primary MC system of the authorized user shares a user profile for the authorized user with any partner MC systems which are providing service to MC service users that are (potential) targets for discreet listening prior to any requests for discreet listening. According to solution 1, the user profile for the authorized user lists the configured target users for that authorized user. Where there are multiple authorized users who need to perform discreet listening on targets in a partner MC system, a separate user profile is provided to the partner MC system for each of those authorized users. The profiles are provided to the MC service servers providing service to the target MC service users, so that requests for discreet listening can be authorized when needed.

The additional information in the user profile of the authorized user is shown in table 6.5.1.2.3-1 below, and is the same as that shown in Solution 1.

Table 6.5.1.2.3-1: Addition to user profile (on network) for authorized user

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Reference | Parameter description | MCPTT UE | MCPTT Server | Configuration management server | MCPTT user database |
|  | Authorized to perform discreet listening on another MC service user | Y | Y | Y | Y |
|  | List of users upon whom discreet listening can be invoked |  |  |  |  |
|  | > MC service ID | Y | Y | Y | Y |

NOTE: The profile shared with the partner MC system only need contain the information about targets for discreet listening that receive MC service in that partner MC system, and need not contain any other configuration information for the authorized user.

##### 6.5.1.2.4 New configuration table of authorized users – option 3

In this option, a new configuration table is defined in the primary MC system of the authorized users who require discreet listening, which lists those authorized users and each of the valid target users on who discreet listening can be performed. This table is shared with the partner MC system prior to discreet listening taking place. The table is provided to the MC service servers in the partner MC system that provide service to the targets of discreet listening to allow discreet listening invoked by the nominated authorized users to be permitted.

NOTE 1: The MC service server in the primary MC system of the authorized user does not require this table, as the authorization to perform discreet listening and the list of targets is already contained in the user profile for the authorized user.

The form of the table is shown in table 6.5.1.2.4 below.

Table 6.5.1.2.4-1: Table of authorized users for discreet listening for provision to partner MC system

|  |  |  |  |
| --- | --- | --- | --- |
| Reference | Parameter description | MC service server | Configuration management server |
|  | MC service identity of authorized user |  |  |
|  | > MC service ID | Y | Y |
|  | > List of users on who discreet listening can be performed |  |  |
|  | >> MC service ID | Y | Y |

NOTE 2: The primary MC system of the authorized user may provide a configuration table to the partner MC system where only relevant MC service users are listed, i.e. the authorized users that may invoke discreet listening from their primary MC system, and the list of target users that may receive MC service in that partner MC system only.

#### 6.5.1.3 Procedures

Solutions 1 and 2 detail procedures to invoke discreet listening in a single MC system. These procedures can be utilized together with the generic procedures for interconnection which are described in 3GPP TS 23.280 [2] subclause 10.14, which allow the relevant partner MC system to be determined and authorization to be carried out by both primary and partner MC systems.

### 6.5.2 Impacts on existing nodes and functionality

This solution results in additional configuration to be shared between primary MC system of the authorized user and the partner MC system of the authorized user, where the target of discreet listening is receiving MC service in that partner MC system. The nature of the configuration information is determined by which of the three options in subclause 6.5.1.2 is adopted. Configuration information needs to be provided to the MC service servers providing service to the targets of discreet listening so that requests for discreet listening can be authorized. Options 2 and 3 require some examination of the configuration information in the partner system before it is provided to the MC service servers, as the MC service servers to be provided with the configuration information are determined by the lists of users within the configuration tables.

### 6.5.3 Solution Evaluation

This solution expands the solutions 1 and 2 to allow discreet listening where the target is receiving MC service from a different MC system from that of the authorized user performing discreet listening. The three configuration options are evaluated as follow.

- Option 1 adds the list of authorized users to the user profile of every potential target user. This could be considered sensitive, however the target MC service user would not be provided with this aspect of the user profile via the MC service UE, and the list of permissible authorized users does not provide any information about when the discreet listening service is invoked. This option provides the least additional configuration work, as a partner MC system would be configured with this information as a matter of course for any MC service users for who the partner MC system is their primary MC system, and the partner MC system would receive this information whenever an MC service user migrated to that partner MC system. The provision of configuration to MC service server is according to existing procedures.

- Option 2 requires the primary MC system of the authorized user to share a partial user profile with the partner MC system in advance of the invocation of discreet listening. This would be a new set of information which would need to be shared independently from either call related services or migration. Provision to the MC service server in the partner MC system requires analysis of the configuration information, as the target users are members of a lists.

- Option 3 requires a new configuration table to be created and shared by the primary MC system of the authorized users with the partner system in advance of the invocation of discreet listening. As for option 2, this would be a new set of information which would need to be shared independently from either call related services or migration. Provision to the MC service server in the partner MC system requires analysis of the configuration information, as the target users are members of a lists.

Therefore of these three options, option 1 is the most consistent with current MC system operation and requires the least additional configuration work, however options 2 and 3 may result in simpler solutions.

## 6.6 Solution 6: Discreet listening to an MCPTT group

### 6.6.1 Description

#### 6.6.1.1 Overview

This solution serves for the scenario where an authorized user specifies an MCPTT group to be the target of discreet listening. The invocation of discreet listening to a group is based on pre-configured authorizations for the listener and the group members of the target group. The provision of discreet listening of a target group is performed either at the initiation of the group call or during the on-going group call.

#### 6.6.1.2 Configuration

In user profile configuration of MCPTT in TS 23.379 clause A.3, two new parameters are added to indicate the authorization of activating discreet listening to a target group and the list of target groups.

Table 6.6.1.2-1: Addition to MCPTT user profiles (on network)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Reference | Parameter description | MCPTT UE | MCPTT Server | Configuration management server | MCPTT user database |
|  | Authorized to perform discreet listening on an MC service group | Y | Y | Y | Y |
|  | List of group(s) upon which discreet listening can be invoked |  |  |  |  |
|  | > MCPTT group ID(s) | Y | Y | Y | Y |

In group configuraiton data of MCPTT in TS 23.379 clause A.4, a new parameter is added to indicate the authorization of group members for being discreet listened.

Table 6.6.1.2-2: Addition to MCPTT group configuration data (on‑network)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Reference | Parameter description | MCPTT UE | MCPTT Server | Group management server |
|  | >> Authorization for being discreet listened in group communications of this group | N | Y | Y |
|  | >> List of user(s) who are authorized to perform discreet listening to this group |  |  |  |
|  | >>> MCPTT ID(s) | N | Y | Y |

#### 6.6.1.3 Procedures

##### 6.6.1.3.1 Discreet listening activation and deactivation

The procedures for activation and deactivation of discreet listening to groups are shown in figure 6.6.1.3.1-1 and figure 6.6.1.3.1-2 below.



Figure 6.6.1.3.1-1: Discreet listening group activation



Figure 6.6.1.3.1-2: Discreet listening group deactivation

##### 6.6.1.3.2 Provision of discreet listening to groups

The provision of discreet listening can only happen after it is successfully activated. The provision of discreet listening towards a target group is made by inviting the authorized user to the target group call if it is initiated after the activation of discreet listening (as shown in figure 6.6.1.3.2-1), or by transferring the target group call to the authorized user if it is initiated before the activation of discreet listening (as shown in figure 6.6.1.3.2-2).

Pre-conditions:

1. MCPTT client 3 (authorized user) has activated discreet listening to this specified MCPTT group.



Figure 6.6.1.3.2-1: Discreet listening of MCPTT group call (discreet listening for target group is activated)



Figure 6.6.1.3.2-2: Discreet listening of MCPTT group call (discreet listening for target group is not activated)

##### 6.6.1.3.3 Release discreet listening to groups

When the authorized user decides to stop discreet listening to a target group which has no on-going group communications, the discreet listening deactivation procedure is used as defined in subclause 6.6.1.3.1.

When the authorized user decides to stop discreet listening to a target group which has on-going group communications, the procedure as shown in figure 6.6.1.3.3-1 is used. The group communication is unaffected by the release of discreet listening media to the authorized user.



Figure 6.6.1.3.3-1: Release discreet listening to group during on-going communication

0. Media plane for discreet listening to the target MCPTT group has been established.

1-2. The authorized user at MCPTT client 3 requests discreet listening group deactivation to the MCPTT server to stop the target MCPTT group.

3-4. MCPTT server performs discreet listening group call release with the MCPTT client 3.

5. Media plane for discreet listening to the target MCPTT group is released.

When the group call of the target group is released, the discreet listening to the current call is also released as shown in procedure in figure 6.6.1.3.3-2 below.

Pre-conditions:

- The authorized user at MCPTT client 3 is discreet listening to the group call of the target MCPTT group.



Figure 6.6.1.3.3-2: Release discreet listening to current group call at group call release

0. The group call of the target MCPTT group is released.

1-2. MCPTT server performs discreet listening group call release with the MCPTT client 3.

3. Media plane for discreet listening to the target MCPTT group is released.

#### 6.6.1.4 Information flows

The information flows in support of procedures for discreet listening to groups are defined as below.

Table 6.6.1.4-1: Discreet listening group activation request

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MCPTT group ID | M | MCPTT group ID of the target group for discreet listening |

Table 6.6.1.4-2: Discreet listening group activation response

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MCPTT group ID | M | MCPTT group ID of the target group for discreet listening |
| Result | M | Indicates the success or failure of the discreet listening group activation request |

Table 6.6.1.4-3: Discreet listening group deactivation request

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MCPTT group ID | M | MCPTT group ID of the target group to be deactivated for discreet listening |

Table 6.6.1.4-4: Discreet listening group deactivation response

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MCPTT group ID | M | MCPTT group ID of the target group to be deactivated for discreet listening |
| Result | M | Indicates the success or failure of the discreet listening group deactivation request |

Table 6.6.1.4-5: Discreet listening group call request

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MCPTT ID | M | MCPTT ID of the authorized user provisioned with discreet listening (the listener) |
| MCPTT group ID | M | MCPTT group ID of the target group for discreet listening |
| SDP offer | M | Media parameters of MCPTT clients |

Table 6.6.1.4-6: Discreet listening group call response

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MCPTT ID | M | MCPTT ID of the authorized user provisioned with discreet listening (the listener) |
| MCPTT group ID | M | MCPTT group ID of the target group for discreet listening |
| Result | M | Indicates the success or failure of the discreet listening group call request |

Table 6.6.1.4-7: Discreet listening group call release request

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MCPTT ID | M | MCPTT ID of the authorized user provisioned with discreet listening (the listener) |
| MCPTT group ID | M | MCPTT group ID of the target group for discreet listening |

Table 6.6.1.4-8: Discreet listening group call release response

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MCPTT ID | M | MCPTT ID of the authorized user provisioned with discreet listening (the listener) |
| MCPTT group ID | M | MCPTT group ID of the target group for discreet listening |

### 6.6.2 Impacts on existing nodes and functionality

This solution results in the following impacts on existing entities and reference points:

- MCPTT servers and MCPTT clients (of authorized users): addition of functionality for activation and deactivation of discreet listening to a specified target MCPTT group; addition of functionality for provision of discreet listening towards a group call to the authorized user without incorporate this authorized user into the group membership.

- MCPTT user configuration (of authorized user): authorization of invoking discreet listening to a target group and the list of target groups.

- MCPTT group configuration: authorization for being discreet listened in group communications of this group.

- MCPTT-1 reference points: addition of new messages in support of new procedures for discreet listening.

- New procedures to request discreet listening specifying a target MCPTT group and provision of discreet listening to the specified target group.

Editor's note: Solutions are FFS for some regrouping scenarios when transmissions from users or groups that are not targets of discreet listening need to be filtered.

### 6.6.3 Solution Evaluation

This solution supports discreet listening of a target group by using similar mechanisms of discreet listening of a target user defined in Solution 1. This solution has no impact to the existing function models.

## 6.7 Solution 7: Logging of MCData message store and MCData content server

### 6.7.1 Description

#### 6.7.1.1 Overview

This solution addresses key issue 11: logging of MCData content server and message store services.

#### 6.7.1.2 Logging of MCData message store services

A message store provides a private storage facility for an MCData user, where data that has been transmitted or received can be cached for later retrieval, where a message can be saved prior to sending and where data exchanged in a group while the MCData user was not receiving MCData service can be stored in order to provide lossless communications.

As any MCData transactions sent or received can be provided to the MC logging function when transferred, it is not necessary to provide additional logging exchanges between the message store and the MC logging function. However, if logging of MCData content stored in the MCData message store is required, this can be provided as an integral function of the MCData message store, and is therefore out of scope of the present document.

#### 6.7.1.3 Logging of MCData content server transactions

A file distribution transaction involving an MCData content server allows an MCData user to upload a file to an MCData content server, then initiate file transfer to an MCData user or group by sending the URL of the file to the target user or group, and allowing the user or group members to retrieve the file by downloading from the MCData content server. In this solution, the initial file upload is not sent to the MC logging function, but transactions between MCData users to transfer the file are stored in the MC logging function, and the MC logging function can also optionally retrieve the file being exchanged.

NOTE 1: If logging of the file is required when uploaded and before distribution to target users and groups, this can be provided by an integral function of the MCData content server. Such functionality is outside the scope of this solution.

Figure 6.7.1.3-1 illustrates the procedure to log file transfer where an MCData content server is in use.



Figure 6.7.1.3-1: Logging of MCData file distribution using MCData content server

In figure 6.7.1.3-1,

- Steps 1, 2, 3, 4, 6, 8 and 11 follow those for file distribution to a single target MCData user or to a target MCData group, as defined in 3GPP TS 22.282 [5].

- Step 5 alerts the MC logging function to the data transfer following the transmission of the file distribution request to the target users,

- Step 7 informs the MC logging function of the target MCData user or group's response. If the target of the FD operation is a group, a single report message may indicate the responses from multiple group members, and multiple messages may be sent containing the responses from different group members.

NOTE 2: Step 7 may occur before or after steps 6 and/or 8. It is not expected that step 6 or step 8 will be delayed in case of non-receipt of step 7 by the MCData content server, however an implementation may decide to hold or prevent steps 6 and/or 8 taking place in event of delay or non-receipt of step 7 if system policy requires all transactions to be logged, and the requirement for logging overrules the requirement to provide the target MCData users with the file contents.

- The MC logging function may decide (according to configuration) to download and log the content of the file in step 9. Step 9 may also be delayed until after step 11 in which the MC logging function is informed of the download completed report, so that the MC logging function may choose not to download the file unless at least one target user has successfully downloaded the file. Alternatively, the MC logging function may be configured to only log the fact that the file transfer has taken place, and not the file itself, in which case step 9 is omitted.

- Step 11 informs the MC logging equipment of the download complete report(s) of the target user(s) if these are sent. As in step 7, if the target of the FD operation is a group, a single report message may indicate the responses from multiple group members, and multiple messages may be sent containing the responses from different group members.

### 6.7.2 Impacts on existing nodes and functionality

The MCData server needs to send additional messages to the MC logging equipment when MCData file distribution takes place so that the logging recorder can log requests, responses and reports relating to file distribution transactions.

The MCData content server needs to be able to receive requests for file content from the MC logging equipment, in addition to those from the targets of the file distribution transaction.

### 6.7.3 Solution Evaluation

This solution places logging of content stored in an MCData message store out of scope.

This solution provides a solution for logging of MCData file distribution where an MCData content server is in use. Additional functionality is required for the MCData server to inform the MC logging function of file distribution transactions; however this is similar to functionality required between an MCData server and an MCData client for file distribution.

## 6.8 Solution 8: Discreet listening of MCData message store and MCData content server

### 6.8.1 Description

#### 6.8.1.1 Overview

This solution addresses key issue 12: discreet listening of MCData content server and message store services.

#### 6.8.1.2 Discreet listening of MCData message store services

A message store provides a private storage facility for an MCData user, where data that has been transmitted or received can be cached for later retrieval, where a message can be saved prior to sending and where data exchanged in a group while the MCData user was not receiving MCData service can be stored in order to provide lossless communications.

As any MCData transactions sent or received can be provided to the authorized user performing discreet listening when transferred, it is not necessary to provide discreet listening of exchanges between the message store and the MC logging function. However, if discreet listening of MCData content being uploaded to, downloaded from or stored in the MCData message store is required, this can be provided as an integral function of the MCData message store, and is therefore out of scope of the present document.

#### 6.8.1.3 Discreet listening of MCData content server transactions

A file distribution transaction involving an MCData content server allows an MCData user to upload a file to an MCData content server, then initiate file transfer to an MCData user or group by sending the URL of the file to the target user or group, and allowing the user or group members to retrieve the file by downloading from the MCData content server. In this solution, the initial file upload is not notified or sent to the authorized user performing discreet listening, but transactions between MCData users to transfer the file are sent to the authorized user, and the authorized user can also optionally retrieve the file being exchanged.

NOTE 1: If discreet listening of the file is required when uploaded and before distribution to target users and groups, this can be provided by an integral function of the MCData content server. Such functionality is outside the scope of this solution.

Figure 6.8.1.3-1 illustrates the procedure for discreet listening where an MCData content server is in use. In this procedure, at least one of the sourcing MCData client 1 or the target MCData users or groups are the target for the discreet listening service. The authorized user is making use of MCData client 2 to perform the discreet listening service.



Figure 6.8.1.3-1: Discreet listening of MCData file distribution using MCData content server

In figure 6.8.1.3-1,

- Steps 1, 2, 3, 4, 7, 10 and 12 follow those for file distribution to a single target MCData user or to a target MCData group, as defined in 3GPP TS 22.282 [5].

- Step 5 alerts the authorized user at MCData client 2 to the request for data transfer sent to the target users, and step 6 contains the response from MCData client 2 informing the MCData server that MCData client 2 received the MCData FD discreet listening request.

NOTE 2: Step 6 may occur before or after step 7. However, the MCData server should not cause the file download in step 10 to be delayed or impeded if step 7 is not received by the MCData server, to prevent the discreet listening service from causing any perceived change to the MCData FD service to the users taking part in the FD service.

- Step 8 informs the authorized user at MCData client 2 of the target MCData user or group's response and step 9 contains the response from MCData client 2 confirming receipt of the target user or group's response by MCData client 2. If the target of the FD transfer is a group, a single message may contain the responses of multiple users, and multiple messages may be sent indicating the responses of multiple group members.

- The authorized user may choose to download the specified file contents in step 11.

NOTE 3: The file needs to be stored in the MCData content server long enough to enable the authorized user to retrieve the file.

- Step 13 informs the authorized user at MCData client 2 of the download complete report(s) of the target user(s) if these are sent, and step 14 confirms receipt of this to the MCData server. As for step 8, a single discreet listening report sent to MCData client 2 in step 13 may contain reports from multiple target MCData group members, and multiple messages may be sent in step 13.

NOTE 4: Steps 6, 9 and 14 may utilise an automatic process, such that a human user does not need to make a decision at the time that the file download commences.

### 6.8.2 Impacts on existing nodes and functionality

The MCData server needs to send additional messages to the MCData client of the authorized user relating to file distribution transactions.

The MCData content server needs to be able to and authorized to receive requests for file content from the MCData client of the authorized user, in addition to those from the targets of the file distribution transaction. Such download of content is not visible to the originator of the content, or the target recipients of the content.

Additional configuration will be needed to achieve this functionality.

### 6.8.3 Solution Evaluation

This solution places discreet listening of content stored in an MCData message store out of scope.

This solution provides a solution for discreet listening of MCData file distribution where an MCData content server is in use. Additional functionality is required for the MCData server to inform the MCData client of the authorized user of file distribution transactions; however this is similar to functionality required between an MCData server and an MCData client for file distribution.

## 6.9 Solution 9: Functionality for discreet listening with regulatory constraints and operator security policies

### 6.9.1 Description

#### 6.9.1.1 Functional model

Discreet listening is carried out by an authorized user, who requests discreet listening for the communications of another user or several users. There is no differentiation to the type of communication, e.g. individual or group communications. The authorized user will require a client entity capable of fulfilling the discreet listening request. The functionality required is the same as that of an MC service client, with the addition of the capability to request discreet listening and specify an MC service user or several MC service users as target. In contrast to discreet listening with no constraints, discreet listening with regulatory constraints and operator security policies is only applied to an MC service user or several MC service users, which are identified as target MC service user(s). The communications of other MC service users which are not defined as targets are not available to the requested authorized MC service user.

This solution addresses aspects of key issue 14, Limitations on discreet listening due to regulatory constraints and operator security policies.

#### 6.9.1.2 Configuration

The user profiles for MCPTT, MCVideo and MCData which are specified in 3GPP TS 23.379 [7], 3GPP TS 23.281 [8] and 3GPP TS 23.282 [9] will need additional configuration to be added as shown in Table 6.9.1.2-1 below.

Table 6.9.1.2-1: Addition to MC service user profiles (on network)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Reference | Parameter description | MC service UE | MC service Server | Configuration management server | MC service user database |
|  | Authorized to perform discreet listening on another MC service user | Y | Y | Y | Y |
| [R-6.15.1-003] of 3GPP TS 22.280 [2] | List of users upon whom discreet listening can be invoked |  |  |  |  |
|  | > MC service ID (see NOTE 1) | Y | Y | Y | Y |
|  | > Limited communication (see NOTE 2) | Y | Y | Y | Y |
| NOTE 1: Due to regulatory constraints and operator security policies only MC service IDs are provided, which are identified as targets.  NOTE 2: If applicable, only the originating transmissions of the target MC service ID is available. Otherwise communications from and to the target will be part of discreet listening. | | | | | |

In Table 6.9.1.2-1 'MC service' represents one of MCPTT, MCVideo or MCData.

#### 6.9.1.3 Procedures

##### 6.9.1.3.1 General

New procedures are added to allow the MC service client of the authorized user to invoke and revoke discreet listening of an MC service user or several MC service users identified as target(s), and to allow the MC service server to provide the content of communications in which the target MC service users are involved. Communications of a MC service user or several MC service users not identified as targets are not available to the requested authorized MC service user.

##### 6.9.1.3.2 Discreet listening invocation and revocation procedures

The procedure allows the MC service client of the authorized user to request discreet listening of a target MC service user. The procedure is illustrated in Figure 6.9.1.3.2-1 below.



Figure 6.9.1.3.2-1: Discreet listening invocation

The information flows needed to support such a procedure are shown in tables 6.9.1.3.2-1 and 6.9.1.3.2-2 below.

Table 6.9.1.3.2-1: Discreet listening activation request

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MC service ID (NOTE) | M | MC service ID of the target of the discreet listening request |
| NOTE: Due to regulatory constraints and operator security policies only a MC service ID is provided, which is identified as target. | | |

Table 6.9.1.3.2-2: Discreet listening activation response

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MC service ID (NOTE) | M | MC service ID of the target of the discreet listening request |
| Result | M | Indicates the success or failure of the discreet listening request |
| NOTE: Due to regulatory constraints and operator security policies only a MC service ID is provided, which is identified as target. | | |

A similar procedure, not illustrated here, is required for revocation of the discreet listening function.

##### 6.9.1.3.3 Provision of discreet listening content for private communications

When the target user makes or receives a private call or initiates individual communications with a server, the authorized user needs to be informed and provided with the media. Figure 6.9.1.3.3-1 below illustrates a procedure where discreet listening target MC service client 1 sets up a call.



Figure 6.9.1.3.3-1: Discreet listening of target initiated private call

Steps 1 to 7 follow those in solution 1, subclause 6.1.1.3.3.

When the target MC service client 1 sends media (step 8a) to the called party MC service client 2 (step 8b), the media is also sent to the authorized user MC service client 3 (step 8c) by the MC service server,

However, when the called party MC service client 2, who is outside the scope of the constrained discreet listening service, sends media (step 9a) to the target MC service client 1 (step 9b), media is not forwarded to the authorized user MC service client 3.

The procedure is similar if the target of the discreet listening is the recipient of the private call.

NOTE 1: If the MC service server does not receive the 'discreet listening call response' for any reason, the call should still proceed so that the requirement that the call is not affected and the target user is not aware of the discreet listening process is satisfied.

NOTE 2: Under certain circumstances, the authorized user may also receive communications of the other party in the communication, e.g. due to imperfect echo cancellation in calls without floor control.

##### 6.9.1.3.4 Provision of discreet listening content for group communications

When the target user makes or receives a group call, the authorized user needs to be informed and provided with the media. Figure 6.9.1.3.4-1 below illustrates a procedure where discreet listening target MC service client 2 is a receiving party in a group call initiated by another affiliated group member.



Figure 6.9.1.3.4-1: Discreet listening of target initiated group call

The procedure is similar if the target of the discreet listening is the initiator of the group call.

NOTE 1: If the MC service server does not receive the 'discreet listening call response' for any reason, the call should still proceed so that the requirement that the call is not affected and the target user is not aware of the discreet listening process is satisfied.

NOTE 2: It is irrelevant whether the authorized user is or is not a member of the MC service group.

##### 6.9.1.3.5 Information flows for discreet listening

Identical to solution 1, subclause 6.1.1.3.5.

### 6.9.2 Impacts on existing nodes and functionality

This solution results in the following impacts on existing entities and reference points:

- Similar impacts as described in solution 1, subclause 6.1.3.

In each case, MC service is one of MCPTT, MCVideo or MCData.

### 6.9.3 Solution Evaluation

This solution allows discreet listening with regulatory constraints and applied operator security policies to be achieved with minimal changes to the functional model as it only requires enhancement to existing functional entities and reference points. It also allows discreet listening to be invoked on a service dependent basis as it is achieved as a function of the MC service specific MC service clients.

## 6.10 Solution 10: Functionality for on-network logging and replay

### 6.10.1 Description

#### 6.10.1.1 Functional model

To support on-network logging and replay, existing common service core functional entities are reused.

The MC logging function makes use of a new MC logging client which has a subset of the functionality of an existing MC service client, in that it can receive communications information and communications content relating to logged users, but cannot set up calls or demand to take part in calls. Provision of call related information and call content is achieved by configuration in the MC service server. The MC logging client uses an MC service ID to allow call related information and call content to be routed to the MC logging client, reusing functionality from existing reference points.

NOTE 1: An MC logging function may contain multiple MC service clients to allow the separate services MCPTT, MCVideo and MCData to be logged within the same function. However this is out of scope of the description of the functional model.

Figure 6.10.1.1-1 below illustrates the functional entities and reference points of the common services core in the application plane that are used for logging.



Figure 6.10.1.1-1: Common services core functional model for logging

The difference to solution#3 is listed as below:

1. The MC replay function receives the necessary security information (e.g., keys used to decrypt the signalling information and media if the solution is intended to log communications with any end to end encryption removed) needed to replay logged communications via MCLog-11 from MC Logging function. A user of the replay function, or an automatic function of the replay function, will perform the necessary authorizations to retrieve logged communications, and MCLog-11 will be used to verify the authenticity and authorization of the user or function.

2. The interface MCLog-10 is used for the MC replay client to access logged communications from logging storage in MC logging function.

3. MCLog-10 and MCLog-11 do not need to use 3GPP access for connectivity, and are outside the scope of this solution.

Figure 6.10.1.1-2 below shows the MC service related application plane entities used to log communications.



Figure 6.10.1.1-2: MC service related application plane functional model for logging

The description MC service related application plane functional model for logging is the same as described in solution#3.

#### 6.10.1.2 Configuration

The configuration aspect is the same as described in solution#3.

#### 6.10.1.3 Procedures

The procedures to enable MC logging function is the same as described in solution#3.

The MC replay equipment and the interfaces MCLog-10, MClog-11 are outside scope of this solution.

### 6.10.2 Impacts on existing nodes and functionality

New entities are introduced in this solution, specifically the MC logging equipment and its constituent MC logging client together with MC logging storage and the MC replay equipment containing the MC replay client. The new MC logging client is based on existing MC service clients to maximise reuse of existing functionality and reference points.

The process for authentication and service authorization use existing functional entities, reference points and procedures.

New configuration will be introduced to configure logging equipment, and to configure MC service groups with the list of MC logging equipment that will log MC service group communications.

New procedures for logging call related information and call contents will be required. However these can be based on existing procedures for call setup and floor, transmission and media control within calls.

Interactions between MC logging client, logging storage and the MC replay client are not specified within this solution and so have no impact on existing nodes and functionality.

### 6.10.3 Solution Evaluation

This solution defines new functional entities and reference points to fulfil the on-network logging requirement together with reuse of existing common services core functional entities and reference points. The new functional entities and reference points will be based on the functionality of existing MC service clients and associated reference points.

The interaction between the MC replay client and the MC logging function is outside the scope of the present document.

A set of procedures will need to be defined to show the invocation of logging functions on logged calls.

# 7 Overall Evaluation

## 7.1 General

The following subclauses contain an overall evalation of the solutions presented in this technical report, and their applicability to the key issues raised. Subclause 7.2 provides an evaluation of the solutions provided in clause 6, and their impact on other entities and working groups, and shows the mapping of the solutions to the key issues outlined in clause 5. Subclause 7.3 lists the key issues with security implications that will need consideration in 3GPP SA WG3.

## 7.2 Solution evaluation

Table 7.2-1 below shows the mapping of key issues to solutions.

Table 7.2-1: Mapping of key issues to solutions

|  |  |
| --- | --- |
| Key issue | Solution |
| 1: Selection of MC service for discreet listening | Solution #1: Functionality for discreet listening |
| 2: Group membership of authorized MC user for discreet listening | Solution #1: Functionality for discreet listening |
| 3: Discreet listening for MCVideo push and pull and MCData file upload and download | Solution #2: Discreet listening of MCVideo push and pull |
| 4: Discreet listening of end to end encrypted calls | Out of scope (see note) |
| 5: Logging and replay of end to end encrypted calls | Out of scope (see note) |
| 6: Source MC service server for discreet listening of user in group call | Solution #1: Functionality for discreet listening |
| 7: Discreet listening and logging for interconnected MC system | Solution #4: On-network logging for interconnection and migration  Solution #5: Discreet listening for interconnection and migration |
| 8: Discreet listening and logging for migrated MC service user | Solution #4: On-network logging for interconnection and migration  Solution #5: Discreet listening for interconnection and migration |
| 9: Discreet listening and logging for user receiving MC service on multiple devices | Solution #1: Functionality for discreet listening  Solution #2: Discreet listening of MCVideo push and pull  Solution #3: Functionality for on-network logging and replay |
| 10: Logging of MC service users and MC service groups | Solution #3: Functionality for on-network logging and replay  Solution #10: Functionality for on-network logging and replay |
| 11: Logging of MCData content server and message store services | Solution #7: Logging of MCData message store and MCData content server |
| 12: Discreet listening of MCData content server and message store services | Solution #8: Discreet listening of MCData message store and MCData content server |
| 13: Discreet listening towards an MC service group | Solution #6: Discreet listening to an MCPTT group |
| 14: Limitations on discreet listening due to regulatory constraints and operator security policies | Solution #9: Functionality for discreet listening with regulatory constraints and operator security policies |
| NOTE: Security solutions are within the remit of SA3 | |

The solutions specified in this technical report are described in table 7.2-2, together with the evaluation text for each solution.

Table 7.2-2: Solution evaluations

| Solution | Applicable key issues | Evaluation | Impact on other entities and working groups |
| --- | --- | --- | --- |
| Solution 1: Functionality for discreet listening | 1: Selection of MC service for discreet listening  2: Group membership of authorized MC user for discreet listening  6: Source MC service server for discreet listening of user in group call  9: Discreet listening and logging for user receiving MC service on multiple devices | This solution allows discreet listening to be achieved with minimal changes to the functional model as it only requires enhancement to existing functional entities and reference points. It also allows discreet listening to be invoked on a service dependent basis as it is achieved as a function of the MC service specific MC service clients. It supports the situations where the MC service user is receiving MC service on multiple MC service clients. | Minor impact on downstream groups to add functionality to existing functional entities and reference points. |
| Solution 2: Discreet listening of MCVideo push and pull | 3: Discreet listening for MCVideo push and pull and MCData file upload and download  9: Discreet listening and logging for user receiving MC service on multiple devices | This solution allows discreet listening of MCVideo push and pull transactions to be achieved with minimal changes to existing MCVideo functionality, as the provision of discreet listening is based on existing MCVideo push and pull procedures. The solution includes a means of identifying the MCVideo client where an MCVideo user is receiving MCVideo service from multiple MCVideo clients. Additional configuration parameters are likely to be needed to support the service. | Minor impact on downstream groups to add functionality to existing functional entities and reference points. |
| Solution 3: Functionality for logging and replay | 10: Logging of MC service users and MC service groups  9: Discreet listening and logging for user receiving MC service on multiple devices | This solution defines new functional entities and reference points to fulfil the on-network logging requirement together with reuse of existing common services core functional entities and reference points. The new functional entities and reference points will be based on the functionality of existing MC service clients and associated reference points. The solution includes a means of identifying the MC service client where an MC service user is receiving MC service from multiple MC service clients.  A set of procedures will need to be defined to show the invocation of logging functions on logged calls. | Impact on downstream groups to add new functionality, based on existing call related functionality. |
| Solution 4: On-network logging for interconnection and migration | 7: Discreet listening and logging for interconnected MC system  8: Discreet listening and logging for migrated MC service user | This solution expands the solution defined in solution 3 to allow logging where the logging equipment is providing logging services in a different MC system to that of the MC logging equipment.  Three options are provided to provide configuration to a partner MC system to enable logging of individual communications. Of these, option 1 which adds the MC service ID associated with the MC logging equipment to the user profile is preferred as it does not add further configuration tables to be exchanged between primary and partner MC systems to enable interconnection and migration, and does not require any analysis in the partner MC system to determine which MC service servers need to be provided with the information. | Impact on downstream groups to add parameters to configuration tables. |
| Solution 5: Discreet listening for interconnection and migration | 7: Discreet listening and logging for interconnected MC system  8: Discreet listening and logging for migrated MC service user | This solution expands the solutions 1 and 2 to allow discreet listening where the target is receiving MC service from a different MC system from that of the authorized user performing discreet listening. Three configuration options are provided to enable discreet listening. Of these three options, option 1 is the most consistent with current MC system operation and requires the least additional configuration work, however options 2 and 3 may result in simpler solutions. | Impact on downstream groups to add parameters to configuration tables, or to create new configuration tables. |
| Solution 6: Discreet listening to an MCPTT group | 13: Discreet listening towards an MC service group | This solution supports discreet listening of a target group by using similar mechanisms of discreet listening of a target user defined in Solution 1. This solution has no impact to the existing function models. | Minor impact on downstream groups to add functionality to existing functional entities and reference points. |
| Solution 7: Logging of MCData message store and MCData content server | 11: Logging of MCData content server and message store services | This solution provides a solution for logging of MCData file distribution where an MCData content server is in use. Additional functionality is required for the MCData server to inform the MC logging function of file distribution transactions; however this is similar to functionality required between an MCData server and an MCData client for file distribution. | Impact on downstream groups to add new functionality, based on existing MCData server to client functionality. |
| Solution 8: Discreet listening of MCData message store and MCData content server | 12: Discreet listening of MCData content server and message store services | This solution provides a solution for discreet listening of MCData file distribution where an MCData content server is in use. Additional functionality is required for the MCData server to inform the MCData client of the authorized user of file distribution transactions; however this is similar to functionality required between an MCData server and an MCData client for file distribution. | Impact on downstream groups to add new functionality, based on existing MCData server to client functionality. |
| Solution 9: Functionality for discreet listening with regulatory constraints and operator security policies | 14: Limitations on discreet listening due to regulatory constraints and operator security policies | This solution allows discreet listening with regulatory constraints and applied operator security policies to be achieved with minimal changes to the functional model as it only requires enhancement to existing functional entities and reference points. It also allows discreet listening to be invoked on a service dependent basis as it is achieved as a function of the MC service specific MC service clients. | Impact on downstream groups to add new functionality, based on existing call related functionality. |
| Solution 10: Functionality for on-network logging and replay | 10: Logging of MC service users and MC service groups | This solution defines new functional entities and reference points to fulfil the on-network logging requirement together with reuse of existing common services core functional entities and reference points. The new functional entities and reference points will be based on the functionality of existing MC service clients and associated reference points.  The interaction between the MC replay client and MC logging function is outside the scope of the present document.  A set of procedures will need to be defined to show the invocation of logging functions on logged calls. | Impact on downstream groups to add new functionality, based on existing call related functionality. |

## 7.3 Key issues with security implications

The following key issues have security considerations that will need review and possible solutions by SA3:

- Key issue 4: Discreet listening of end to end encrypted calls; and

- Key issue 5: Logging and replay of end to end encrypted calls.

# 8 Conclusions

This technical report presents scenarios, key issues and solutions for discreet listening and logging for MC services.

All key issues that are addressed by one or more solutions in this Technical Report are presented in subclause 7.2, and those which have security related aspects which are considered to be outside the scope of solutions within this Technical Report are presented in subclause 7.3.

The set of solutions described in this Technical Report are candidate solutions for normative work. These solutions provide updates to the functional models for MC services that will permit discreet listening and logging to be realised, configuration which will permit discreet listening and logging services to be achieved and describe the essentials of procedures to provide the services themselves.

Some key issues and some solutions have security considerations. These are identified in clause 7.

# Annex A: Reproduction of stage 1 requirements

## A.1 Requirements for discreet listening

Requirements listed in this subclause are reproduced from the specifications referenced within this subclause. The referenced specifications are the normative source for the requirements and have precedence over the information reproduced within this subclause.

The requirements in 3GPP TS 22.280 [2] that apply for discreet listening are provided in table A.1‑1. They are applied to all services MCPTT, MCVideo and MCData according to the reference tables in Annexes A, B and C of [2].

Table A.1-1: Discreet listening requirement

|  |  |
| --- | --- |
| Requirement | Description |
| [R-6.15.1-001a] | The MCX Service shall provide discreet listening capabilities without noticeable impact on or knowledge of the target MCX User, or the members of the target MCX Service Group, and all other unauthorized MCX Users. |
| [R-6.15.1-001] | The MCX Service shall provide a mechanism for an authorized MCX User to receive MCX Service Private Communication transmissions to and from a specific target MCX User that is within the authority of the authorized MCX user. |
| [R-6.15.1-002] | The MCX Service shall provide a mechanism for an authorized MCX User to receive MCX Service Group Communication transmissions to and from a specific target MCX User that is within the authority of the authorized MCX User. |
| [R-6.15.1-003] | Subject to regulatory constraints and operator security policies, the MCX Service shall allow to be configured not to provide transmissions from MCX Users who are communicating with the discreet listening target MCX User, and who are not themselves targets of discreet listening. |
| [R-6.15.1-004] | The MCX Service shall provide a mechanism for an authorized MCX User to receive MCX Service Group transmissions from a specific MCX Service Group that is within the authority of the authorized MCX User. |
| NOTE: Permission to activate discreet listening can include multiple levels of authorization, but this is outside the scope of 3GPP. | |

## A.2 Requirements for recording and audit

Requirements listed in this subclause are reproduced from the specifications referenced within this subclause. The referenced specifications are the normative source for the requirements and have precedence over the information reproduced within this subclause.

The following requirements in 3GPP TS 22.280 [2] for recording and audit are listed in table A.2‑1. They are applied to all services MCPTT, MCVideo and MCData according to the reference tables in Annexes A, B and C of [2].

Table A.2-1: Requirements for recording and audit

|  |  |
| --- | --- |
| Requirement | Description |
| [R-6.15.4-001] | The MCX Service shall provide a mechanism for a Mission Critical Organization to log the metadata of the MCX Service Group Communications and MCX Service Private Communications under the organization's authority. |
| [R-6.15.4-002] | Metadata shall be logged for both the transmitting Participant and the receiving Participant(s). |
| [R-6.15.4-003] | The MCX Service shall provide a mechanism for a Mission Critical Organization to record the transmissions of the Group Communications and Private Communications under the organization's authority. |
| [R-6.15.4-004] | The MCX Service shall provide a mechanism for a Mission Critical Organization to log at least the following metadata per communication: depending on service this may include; start time, date, MCX User ID, MCX Group ID, Location information of the transmitting Participant, end time or duration, end reason, type of communication (e.g., MCX Service Emergency, regroup, private). |
| [R-6.15.4-005] | If an MCX Service Group Communication or MCX Service Private Communication uses end-to-end confidentiality, the MCX Service shall provide a mechanism for a Mission Critical Organization to maintain the end-to-end confidentiality when the MCX Service Group Communication or MCX Service Private Communication is logged. |
| [R-6.15.4-006] | The MCX Service shall provide a mechanism for a Mission Critical Organization to log the metadata of non-communication related user activities under the agency's authority. |
| [R-6.15.4-007] | The MCX Service shall provide a mechanism for a Mission Critical Organization to log at least the following non-communication activity types: MCX Service Emergency Alert, MCX Service Emergency Alert cancellation, In-progress Emergency cancellation, registration state change, overridden event, user remote logout, changing another user's affiliations, affiliation change, and change of Selected MCX Service Group. |
| [R-6.15.4-008] | The MCX Service shall provide a mechanism for a Mission Critical Organization to log at least the following metadata per non-communication activity: time, date, MCX Service User identity, and activity type. The following metadata should be logged if applicable to the activity type: MCX Service Group ID, Location information of the MCX User, affiliation list, target MCX Service User ID and success/failure indication. |
| [R-6.15.4-009] | The MCX Service shall provide a mechanism for a Mission Critical Organization to log metadata for all failed authorization attempts (e.g., invalid login password) by an MCX User. |
| [R-6.15.4-010] | The MCX Service shall provide a mechanism to collect metadata for network access events (e.g., pre-emption of EPS bearer, loss of signal, failed registration attempts). |

The following additional requirement for logging for MCVideo in 3GPP TS 22.281 [3] is provided in table A.2‑2:

Table A.2-2: MCVideo specific requirement for logging

|  |  |
| --- | --- |
| Requirement | Description |
| [R-5.1.10.2-008] | The MCVideo service shall be able to provide an integrity protected timestamped detailed log of all performed and attempted activities for each user of the MCVideo Service. |

Annex B (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2018-05 | SA6 #24 | S6-180761 |  |  |  | TR Skeleton |  |
| 2018-06 | SA6 #24 | S6-180913 |  |  |  | Scope & additional references | 0.1.0 |
| 2018-08 | SA6 #25 | S6-181202 |  |  |  | References and Annex A | 0.2.0 |
| 2018-08 | SA6 #25 | S6-181203 |  |  |  | Definitions and abbreviation | 0.2.0 |
| 2018-08 | SA6 #25 | S6-181204 |  |  |  | Use cases/scenarios general subclause | 0.2.0 |
| 2018-08 | SA6 #25 | S6-181261 |  |  |  | Scenario 1: Discreet listening of MCPTT and MCVideo private calls | 0.2.0 |
| 2018-08 | SA6 #25 | S6-181262 |  |  |  | Scenario 2: Discreet listening of MCPTT and MCVideo group calls | 0.2.0 |
| 2018-08 | SA6 #25 | S6-181263 |  |  |  | Scenario 3: Discreet listening MCVideo pull | 0.2.0 |
| 2018-08 | SA6 #25 | S6-181264 |  |  |  | Scenario 4: Discreet listening MCVideo push | 0.2.0 |
| 2018-08 | SA6 #25 | S6-181265 |  |  |  | Scenario 5: Discreet listening MCData SDS | 0.2.0 |
| 2018-08 | SA6 #25 | S6-181266 |  |  |  | Scenario 6: Discreet listening MCData file distribution | 0.2.0 |
| 2018-08 | SA6 #25 | S6-181211 |  |  |  | Key issue 1: Selection of MC service for discreet listening | 0.2.0 |
| 2018-08 | SA6 #25 | S6-181252 |  |  |  | Key issue 2: Group membership of authorized MC user for discreet listening | 0.2.0 |
| 2018-08 | SA6 #25 | S6-181213 |  |  |  | Key issue 3: Discreet listening for MCVideo push and pull and MCData file upload and download | 0.2.0 |
| 2018-10 | SA6 #26 | S6-181356 |  |  |  | Table titles in Annex A | 0.3.0 |
| 2018-10 | SA6 #26 | S6-181357 |  |  |  | Scenario implemented as scenario 7: Logging scenarios as in subclause 4.8 | 0.3.0 |
| 2018-10 | SA6 #26 | S6-181520 |  |  |  | Key issues implemented as key issue 5.4 in subclause 5.4 and key issue 5.5 in subclause 5.5 | 0.3.0 |
| 2018-10 | SA6 #26 | S6-181521 |  |  |  | Key issue implemented as key issue 6 in subclause 5.6 | 0.3.0 |
| 2018-10 | SA6 #26 | S6-181522 |  |  |  | Key issues implemented as key issue 7 in subclause 5.7 and key issue 8 in subclause 5.8 | 0.3.0 |
| 2018-10 | SA6 #26 | S6-181571 |  |  |  | Implemented as solution 1 in subclause 6.1 | 0.3.0 |
| 2018-12 | SA6 #27 | S6-181799 |  |  |  | Replacement of 'DL' with 'discreet listening' throughout | 0.4.0 |
| 2018-12 | SA6 #27 | S6-181843 |  |  |  | Implemented as solution 2 in subclause 6.2 | 0.4.0 |
| 2018-12 | SA6 #27 | S6-181803 |  |  |  | Update to discreet listening definition | 0.4.0 |
| 2019-01 | SA6 #28 | S6-190122 |  |  |  | Key issue 9 on multiple devices | 0.5.0 |
| 2019-01 | SA6 #28 | S6-190289 |  |  |  | Overall evaluation | 0.5.0 |
| 2019-01 | SA6 #28 | S6-190300 |  |  |  | Solution 3 for logging | 0.5.0 |
| 2019-03 | SA6 #29 | S6-190345 |  |  |  | Key Issue for logging | 0.6.0 |
| 2019-03 | SA6 #29 | S6-190468 |  |  |  | Key Issue for logging MCData services | 0.6.0 |
| 2019-03 | SA6 #29 | S6-190469 |  |  |  | Key Issue for discreet listening of MCData services | 0.6.0 |
| 2019-03 | SA6 #29 | S6-190470 |  |  |  | Group management for logging solution 3 | 0.6.0 |
| 2019-03 | SA6 #29 | S6-190349 |  |  |  | Solution for interconnection & migration for logging | 0.6.0 |
| 2019-03 | SA6 #29 | S6-190471 |  |  |  | Solution for interconnection & migration for discreet listening | 0.6.0 |
| 2019-03 | SA6 #29 | S6-190503 |  |  |  | Key issue for group cased discreet listening | 0.6.0 |
| 2019-03 | SA6 #29 | S6-190528 |  |  |  | Solution for group based discreet listening | 0.6.0 |
| 2019-03 | SA6 #29 | S6-190474 |  |  |  | Update to solution evaluation | 0.6.0 |
| 2019-03 | SA#83 | SP-190061 |  |  |  | Presentation for Information at SA#83 | 1.0.0 |
| 2019-04 | SA6 #30 | S6-190786 |  |  |  | Scenario 8: Limitations on discreet listening due to regulatory constraints and operator security policies | 1.1.0 |
| 2019-04 | SA6 #30 | S6-190787 |  |  |  | Key Issue 14: Limitations on discreet listening due to regulatory constraints and operator security policies | 1.1.0 |
| 2019-04 | SA6 #30 | S6-190564 |  |  |  | Update requirements in Annex A | 1.1.0 |
| 2019-04 | SA6 #30 | S6-190788 |  |  |  | Solution 7: Logging of MCData message store and MCData content server | 1.1.0 |
| 2019-04 | SA6 #30 | S6-190789 |  |  |  | Solution 8: Discreet listening of MCData message store and MCData content server | 1.1.0 |
| 2019-04 | SA6 #30 | S6-190790 |  |  |  | 6.6.1.3.3 Release discreet listening to groups | 1.1.0 |
| 2019-05 | SA6 #31 | S6-190899 |  |  |  | Update solution 1 for multiple UEs | 1.2.0 |
| 2019-05 | SA6 #31 | S6-190900 |  |  |  | Update solution 2 for multiple UEs | 1.2.0 |
| 2019-05 | SA6 #31 | S6-190901 |  |  |  | Update solution 3 for multiple UEs | 1.2.0 |
| 2019-05 | SA6 #31 | S6-191090 |  |  |  | Conclusions | 1.2.0 |
| 2019-05 | SA6 #31 | S6-191091 |  |  |  | Solution 9: Functionality for discreet listening with regulatory constraints and operator security policies | 1.2.0 |
| 2019-05 | SA6 #31 | S6-191201 |  |  |  | Solution 10: Functionality for on-network logging and replay | 1.2.0 |
| 2019-05 | SA6 #31 | S6-191089 |  |  |  | Update overall evaluation | 1.2.0 |
| 2019-05 | SA#84 | S6-190471 |  |  |  | Presentation for Approval | 2.0.0 |
| 2019-06 | SA#84 | S6-190471 |  |  |  | MCC Editorial update for publication after TSG SA approval (SA#84) | 16.0.0 |