|  |  |
| --- | --- |
| 3GPP TR 23.700-38 V18.0.0 (2023-06) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on sharing of administrative configuration between interconnected MC service systems;  (Release 18) | |
|  | |
|  | 3GPP-logo_web |
|  | |
| 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. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2023, 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

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Symbols 9

3.3 Abbreviations 9

4 Scenarios 9

4.1 General 9

4.2 Relationship between MC systems 9

5 Key issues 10

5.1 Key issue 1: functional architecture 10

5.2 Key issue 2 – Identification 11

5.3 Key issue 3 – Change user configuration 11

5.4 Key issue 4 – Group configuration data 11

5.5 Key issue 5 – Service configuration data 11

5.6 Key issue 6: authorization 12

5.7 Key issue 7: Secure exchange and topology hiding 12

6 Architecture requirements 12

6.1 General 12

6.2 Requirements 13

6.2.1 General 13

6.2.1.1 Description 13

6.2.1.2 Requirements 13

6.2.2 User and group authorization 13

6.2.2.1 Description 13

6.2.2.2 Requirements 13

6.2.3 User and group MC service registration 14

6.2.3.1 Description 14

6.2.3.2 Requirements 14

6.2.4 Information and selection of available group communication 14

6.2.4.1 Description 14

6.2.4.2 Requirements 14

6.2.5 Profiles for visiting MC service users 14

6.2.5.1 Description 14

6.2.5.2 Requirements 15

7 Solutions 15

7.1 Common ACM procedure 15

7.1.1 Pending requests 15

7.1.1.1 Solution description 15

7.1.1.1.1 General 15

7.1.1.1.2 Information flows 15

7.1.1.1.3 Procedure 16

7.1.1.2 Solution evaluation 17

7.1.2 Processing incoming requests automatically 17

7.1.2.1 Solution description 17

7.1.2.1.1 General 17

7.1.2.1.2 Automation performed by ACM server 17

7.1.2.1.3 Automation performed by automated ACM client 18

7.1.2.2 Solution evaluation 18

7.2 Mapping of solutions to key issues 19

7.3 Solution #1: Functional architecture 19

7.3.1 Solution description 19

7.3.1.1 General 19

7.3.1.2 Functional model 19

7.3.1.3 Functional entities description 20

7.3.2 Solution evaluation 20

7.4 Solution #2: Enhancement to the MC service functional architecture 20

7.4.1 Solution description 20

7.4.2 Functional model description 20

7.4.3 On-network functional model 20

7.4.4 Administrative configuration management client 21

7.4.5 Administrative configuration management server 22

7.4.6 Administrative configuration management server and client in a primary MC system and partner MC system 22

7.4.7 Solution evaluation 22

7.5 Solution #3: ACMC authorisation 22

7.5.1 Solution description 22

7.5.1.1 Overview 22

7.5.1.1a User profile configurations for using ACMX 23

7.5.1.2 ACMX authorisation for an authorised user 23

7.5.2 Solution evaluation 24

7.6 Solution #4: Group configuration change 24

7.6.1 Solution description 24

7.6.1.1 General 24

7.6.1.2 Procedure 25

7.6.1.2.1 Group membership update by authorized user from a partner MC system 25

7.6.2 Solution evaluation 27

7.7 Solution #5: Request to add users for migration to a partner MC system 27

7.7.1 Solution description 27

7.7.1.1 General 27

7.7.1.2 Information flows 27

7.7.1.2.1 User configuration request 27

7.7.1.2.2 User configuration response 28

7.7.1.3 Procedure 29

7.7.2 Solution evaluation 31

7.8 Solution #6: Request to remove users for migration from a partner MC system 31

7.8.1 Solution description 31

7.8.1.2 Information flows 31

7.8.1.2.1 Remove user configuration request 31

7.8.1.2.2 Remove user configuration response 32

7.8.1.3 Remove user configuration request from a partner MC system 32

7.8.2 Solution evaluation 34

7.9 Solution #7: Update MC service UE initial configuration 34

7.9.1 Solution description 34

7.9.1.1 General 34

7.9.1.2 Information flows 35

7.9.1.2.1 Update MC service UE initial configuration 35

7.9.1.2.2 Update MC service UE initial configuration response 35

7.9.1.3 Procedure 35

7.9.2 Solution evaluation 37

7.10 Solution #8: MC service user profile update request while receiving MC service from a partner MC system 37

7.10.1 Solution description 37

7.10.1.1 General 37

7.10.1.2 Information flows 38

7.10.1.2.1 MC service user profile update request 38

7.10.1.2.2 MC service user profile update response 38

7.10.1.3 Procedure 38

7.10.2 Solution evaluation 40

7.11 Solution #9: Provide Interconnection Group IDs 40

7.11.1 Solution description 40

7.11.1.1 General 40

7.11.1.2 Information flows 40

7.11.1.2.1 Group information provision request 40

7.11.1.2.2 Group information provision response 41

7.11.1.3 Procedure 41

7.11.1.3.1 Authorized user providing interconnection group ID(s) to authorized user of a partner MC system 41

7.11.2 Solution evaluation 43

8 Evaluation 44

8.1 Overview 44

8.2 Overall evaluation of key issue#1 44

8.3 Overall evaluation of key issue#2 44

8.4 Overall evaluation of key issue#3 44

8.5 Overall evaluation of key issue#4 45

8.6 Overall evaluation of key issue#5 45

8.7 Overall evaluation of key issue#6 45

8.8 Overall evaluation of key issue#7 45

9 Conclusions 45

Annex A (informative): Change history 46

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document studies sharing of administrative configuration between interconnected MC service systems, based on stage 1 requirements specified in 3GPP TS 22.280 [2].

This study investigates related use cases and identifies solutions to support exchange administrative configuration, security relevant data and information between interconnected MC service systems.

# 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); Stage 1".

[3] 3GPP TR 22.881: "Study on sharing administrative configuration information between interconnected Mission Critical (MCX) service systems".

[4] 3GPP TS 33.180: "Security of the Mission Critical (MC) service".

[5] 3GPP TS 23.280: "Common functional architecture to support mission critical services; Stage 2".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms 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].

**Administrative Configuration Management eXchange (ACMX):** A term that describes the exchange of administrative configuration management information (e.g. MC service user profile, group management configuration, system parameters) between interconnected MC systems.

**Primary ACMC**: Administrative Configuration Management Client of an MC service user that is homed to the primary MC system.

**Primary ACMS**: Administrative Configuration Management Server of the primary MC system.

**Partner ACMC**: Administrative Configuration Management Client of an MC service user that is homed to partner MC system(s).

**Partner ACMS**: Administrative Configuration Management Server of the partner MC system.

## 3.2 Symbols

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

<symbol> <Explanation>

## 3.3 Abbreviations

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

ACMX Administrative Configuration Management eXchange.

ACMC Administrative Configuration Management Client

ACMS Administrative Configuration Management Server

# 4 Scenarios

## 4.1 General

3GPP TR 22.881 [3] identified some use cases under which the administrative configurations exchange between interconnected MC systems (2 or more MC systems) would typically take place. This will help to identify and specify the solutions aspects in this study, in order to serve these use cases properly.

## 4.2 Relationship between MC systems

Figure 4.2-1 describes the relationship between the interconnected MC systems involved in exchanging the administrative configurations.



Figure 4.2-1: Relationship between interconnected MC systems

An authorized user can trigger the exchange of administrative configurations or/and information with one or more interconnected partner MC system at the same time, which should be regulated through the service agreements with the partner MC systems. The interconnected partner MC systems shall have service agreements to the primary MC system, this is mandatory for this setup. The MC partner systems could potentially have service agreement between them, but this is not relevant for this study.

Processing the configuration data might require the involvement of an authorized user (manually or automatically), who can decide whether to accept, modify or reject the configuration data.

# 5 Key issues

## 5.1 Key issue 1: functional architecture

The support of sharing administrative configurations mechanism in MC service Systems would imply the need to provide new functions and/or sub-functions to the existing MC functional architecture. Defining the overall architecture would help to enhance and develop proper mechanisms, information flows and procedures.

This key issue will:

- Identify the functional architecture enhancements to support this mechanism,

- Describe the details of the single elements from that enhanced architecture.

## 5.2 Key issue 2 – Identification

Performing an ACMX transaction requires to identify the authorized users managing the ACMX in the primary and the partner MC systems, as well as the MC service user(s), i.e. the users require configuration data for migration and/or interconnection.

List of key issues:

- Investigate and clarify, how the authorized users in the primary and the partner MC system are identified, as well the MC service user(s), which are subject of configuration and information exchange between interconnected MC systems.

- Identify the impact on existing solutions.

## 5.3 Key issue 3 – Change user configuration

Migration of MC service users between MC systems may require that their user configuration data to be used in the target partner MC system has been settled prior to attempting requesting MC service there.

List of key issues:

- Investigate and define how to negotiate and agree user profiles (user configuration data) that enable the owner to migrate into a partner MC system.

- Investigate and define methods or mechanisms how an authorised MC service user can request changes for MC service user configuration data in a partner MC system.

## 5.4 Key issue 4 – Group configuration data

The exchange of administrative group configuration data between interconnected MC systems, i.e. between a primary MC system and one or more partner MC systems needs specifying.

Solutions are required that enable the exchange of administrative group configuration data between interconnected MC systems.

List of key issues:

- Investigate and develop solutions, if required, which enable the exchange of administrative group configuration data between interconnected MC systems, which are not yet currently available.

- Investigate and develop solutions, if required, which enable requesting changes, such as adding or deleting group configuration data for MC service users located in one or more partner MC systems.

Investigate and develop solutions, if required, which enable the exchange/request of information relating to group configuration for MC service users located in one or more partner MC systems.

## 5.5 Key issue 5 – Service configuration data

The exchange of administrative service configuration data between interconnected MC systems, i.e. between a primary MC system and one or more partner MC systems needs specifying.

Solutions are required that enable the exchange of administrative service configuration data between interconnected MC systems.

List of key issues:

- Investigate and develop solutions, if required, which enable the exchange of administrative service configuration data between interconnected MC systems, which are not yet currently available.

- Investigate and develop solutions, if required, which enable requesting changes, such as adding or deleting service configuration data for MC service users located in one or more partner MC systems.

- Investigate and develop solutions, if required, which enable the exchange/request of information relating to service configuration for MC service users located in one or more partner MC systems.

## 5.6 Key issue 6: authorization

For sharing administrative configurations, an authorized user in the primary MC system should be enabled to use this service; where this user should have the corresponding/sufficient access rights to perform the required actions to serve a certain use case.

For providing different access permissions to different authorized users, some access control components could be used to determine the level of authorization of each user. In addition, access control components could help to manage requests and information exchange and to track the access activities for user(s) to ensure their accountability for the performed actions under different circumstances.

The involved MC systems operate independently, using control entities for connecting and exchanging the administrative data, where these control entities manage the parameters exchange at their own MC system entities/servers.

This key issue will:

- Clarify how to reuse or enhance available methods to authorize an administrator or authorized user at primary system and;

- clarify how to authorize the exchange between MC systems.

- Investigate whether and how the different scenarios/use cases could influence the authorization level for that user(s).

NOTE 1: The authorized user is not a migrated MC service user in partner MC system, and is not changing the configurations directly in partner MC system

NOTE 2: Procedures for authentication/authorization for MC service user(s) in inter-domain and/or migrating are defined in 3GPP TS 33.180 [4].

## 5.7 Key issue 7: Secure exchange and topology hiding

Administrative configurations exchange is performed between MC systems, sharing the same security domain, or are located in different security domains. This would imply the need to ensure a secure exchange between MC systems, and at the same time without exposing the network topology of involved MC systems.

This key issue will:

- Investigate and clarify how to perform administrative configuration exchange without compromising the integrity and security of the involved MC systems.

- Investigate and clarify how to perform administrative configuration exchange without exposing the network topology of either MC systems.

# 6 Architecture requirements

## 6.1 General

This clause provides a general description of enhancements to the architecture requirements.

## 6.2 Requirements

### 6.2.1 General

#### 6.2.1.1 Description

This clause specifies the general requirements for functional architecture.

#### 6.2.1.2 Requirements

[AR-6.2.1.2-01] An authorized user of an MC system shall be able to exchange administrative configuration parameters and device information with one or more partner MC system(s) at the same time.

[AR-6.2.1.2-02] An authorized user of an MC system shall have the capability to address partner MC system(s) by a worldwide unique identity.

[AR-6.2.1.2-03] An authorized user of an MC system shall have appropriate access to setup, initiate, authorize, verify and review interconnection and migration requests between the primary MC system and the partner MC system(s).

[AR-6.2.1.2-04] The MC system receiving administrative configuration and information requests shall have the capability to react to the requests.

[AR-6.2.1.2-05] MC system receiving a particular request shall be able to notify the requesting MC system, including a result for this request.

[AR-6.2.1.2-06] An authorized user of an MC system shall be able to request information from partner MC system about its available functionalities and offered MC services.

[AR-6.2.1.2-07] MC system shall be able to provide information about its available functionalities and offered MC services.

[AR-6.2.1.2-08] Exchange of information between MC systems shall not compromise the security of either MC system.

[AR-6.2.1.2-09] Exchange of information shall not expose the internal structure or configuration of either MC system.

### 6.2.2 User and group authorization

#### 6.2.2.1 Description

This clause specifies the requirements for MC service user and group authorization by their primary MC system and the partner MC system(s) for interconnection and migration.

#### 6.2.2.2 Requirements

[AR-6.2.2.2-01] The MC system shall be able to verify that the migration or interconnection request is permitted (i.e. either by the primary MC system or by partner MC system, or by both MC systems) for that MC service user.

[AR-6.2.2.2-02] The primary MC system may change or restrict the MC services available to MC service user(s) which are provided by the system for interconnection to particular partner MC system(s).

[AR-6.2.2.2-03] The MC system shall be able to authorize an incoming migration or interconnection request from a particular MC service user.

NOTE: Examples of such requests may include affiliation to groups or a specific group, to receive a list of interconnection groups and/or, being added to a group or groups.

[AR-6.2.2.2-04] The MC system shall be able to provide a user profile for a migrated MC service user, which may change the authorizations compared with the authorizations that the MC service user has for the same MC service within the primary MC system.

### 6.2.3 User and group MC service registration

#### 6.2.3.1 Description

This clause specifies the requirements for MC service user and group service registrations with partner MC system(s).

#### 6.2.3.2 Requirements

[AR-6.2.3.2-01] The MC system shall be able to request a list of interconnecting groups from partner MC system(s).

[AR-6.2.3.2-02] The MC system shall be able to react to group modification requests from a partner MC system(s).

[AR-6.2.3.2-03] The MC system shall be able to send a list of MC service user ID's, including MC UE identification, that are proposed to be added as group members in an interconnecting group to a partner MC system.

NOTE 1: The MC service UE label could be used as an UE identification element, for example.

[AR-6.2.3.2-04] The MC system shall be able to receive a list of MC service user ID's, including MC UE identification, that are proposed to be added as group members in an interconnecting group from partner MC system(s).

NOTE 2: The MC service UE label could be used as an UE identification element, for example.

### 6.2.4 Information and selection of available group communication

#### 6.2.4.1 Description

This clause specifies the requirements for MC service user information and selection of available group communications between interconnected partner MC system(s).

#### 6.2.4.2 Requirements

[AR-6.2.4.2-01] The MC system shall have the capability to provide information about available group communications, which can lead to a participation request.

[AR-6.2.4.2-02] The MC system shall have the capability to configure MC Service User privileges to request information about available groups from partner MC system(s).

[AR-6.2.4.2-03] An authorized user shall be able, based on the users individual privileges, to request information about currently active and available group communications from partner MC system(s).

[AR-6.2.4.2-04] An authorized user shall be able to request affiliation to groups and/or currently active groups, available to the user and based on the users individual privileges, from partner MC system(s).

[AR-6.2.4.2-05] An MC service user shall be able to receive pushed information about available groups, based on individual privileges, from partner MC system(s).

NOTE 1: Pushed information is information provided without sending a specific request prior. This may be required for automatic notification if new and relevant groups for a specific incident become available.

[AR-6.2.4.2-06] An MC system receiving the group affiliation request shall have the capability to notify of a successful or denied affiliation request, from partner MC system(s).

NOTE 2: Notification could be provided to the requesting MC service user or alternatively to authorised MC service users, such as dispatchers, for example.

### 6.2.5 Profiles for visiting MC service users

#### 6.2.5.1 Description

This clause specifies the requirements for profiles for visiting MC service users migrating from their primary MC system into an interconnected partner MC system.

#### 6.2.5.2 Requirements

[AR-6.2.5.2-01] MC system shall have the capability to pre-arrange visitor user profiles.

[AR-6.2.5.2-02] MC system shall be able to provide a user profile for a visiting MC service user.

[AR-6.2.5.2-03] MC system which hosts migrated MC service user shall have authority over the MC service user profile changes, affecting its system.

[AR-6.2.5.2-04] MC system shall have the capability to exchange additional MC service user information with the MC service user's home MC system.

# 7 Solutions

## 7.1 Common ACM procedure

### 7.1.1 Pending requests

#### 7.1.1.1 Solution description

##### 7.1.1.1.1 General

This clause provides a description of the common ACM procedure and the related information flows used in other solutions. This procedure provides the detailed description of the steps that are not included in other solutions for simplicity.

This solution is not related to any specific key issue.

##### 7.1.1.1.2 Information flows

7.1.1.1.2.1 ACM data notification

Table 7.1.1.1.2.1-1 describes the information flow of the ACM data notification from a ACM server to the ACM client.

Table 7.1.1.1.2.1-1: ACM data notification

|  |  |  |
| --- | --- | --- |
| **Information element** | **Status** | **Description** |
| MC service ID | M | The identity of the MC service user towards which the pending ACM data notification is sent |

7.1.1.1.2.2 Get ACM data request

Table 7.1.1.1.2.2-1 describes the information flow of Get ACM data request from an ACM client to the ACM server.

Table 7.1.1.1.2.2-1: Get ACM data request

|  |  |  |
| --- | --- | --- |
| **Information element** | **Status** | **Description** |
| MC service ID | M | The identity of the MC service user requesting for the download of the pending ACM data (The ACM data corresponds to the user for later delivery) |

7.1.1.1.2.3 Get ACM data response

Table 7.1.1.1.2.3-1 describes the information flow of Get ACM data response from an ACM server to the ACM client.

Table 7.1.1.1.2.3-1: Get ACM data response

|  |  |  |
| --- | --- | --- |
| **Information Element** | **Status** | **Description** |
| MC service ID | M | The identity of the MC service user requesting for the download of the pending ACM data (The ACM data corresponds to the user for later delivery) |
| ACM Data  (NOTE) | M | Contains all ACM data that is pending for this user. |
| NOTE: ACM Data can contain a priority which indicates the urgency of each individual pending ACM data element (e.g. priority can be high, medium, low for specific urgency). | | |

##### 7.1.1.1.3 Procedure

Upon receiving an ACM request the ACM server should forward the request to the authorized user at its MC system. Performing this process might require considerable waiting time if the target authorized user is not logged on.

In addition, when an ACM server receives a response to a previously sent ACM request, where the authorized user is not logged on, the ACM server should store the response and notify the authorized user when the user logs on again.

The common procedure for pending ACM request/response is shown in figure 7.1.1.1.3-1

Pre-conditions

- The ACM server has received an ACM request, or a response, and has stored it.

- The ACM server has received an ACM request that should be validated by an authorized user

- The targeted ACM authorized user is currently not logged on.



Figure 7.1.1.1.3-1: Pending requests Procedure

1. An authorized MC service user of the MC system logs on to the ACM client.

2. The ACM server notifies the ACM client of the pending ACM data.

3. The ACM client requests the ACM server to send the pending ACM data.

4. The ACM server sends the stored ACM data to the ACM client.

NOTE: when this procedure referenced in other solutions, the individual ACM request/response information flows are provided by the related procedures in details.

#### 7.1.1.2 Solution evaluation

This solution provides a common procedure for handling stored ACM requests and responses from partner MC systems.

### 7.1.2 Processing incoming requests automatically

#### 7.1.2.1 Solution description

##### 7.1.2.1.1 General

This solution provides the possibility of managing and responding to the incoming requests automatically. It describes the automation options performed in the ACM server or by an automated ACM client.

##### 7.1.2.1.2 Automation performed by ACM server

The partner ACM server verifies the request and send a response to the primary MC system. Automation performed by ACM server shown in Figure 7.1.2.1.2-1.



Figure 7.1.2.1.2-1: Automation performed by ACM server

The following applies:

- The partner ACM server audits the request and decides whether to apply the configurations or not.

- The partner ACM server takes whatever actions are needed to apply the configurations to the partner MC system. The actions within the partner MC system to apply the configurations, including the interaction with other servers, are outside the scope of the 3GPP specification

- The partner ACM server provides the possibility for the authorized users in the partner MC system to update the automation rules, or to terminate this automation, if required.

- The partner ACM server provides tracking mechanism for the authorized users in the MC system for all automatically performed actions.

##### 7.1.2.1.3 Automation performed by automated ACM client

The ACM server sends the received request to an automated ACM client for processing and sending a response automatically to primary MC system without human interaction, as shown figure 7.1.2.1.3-1.



Figure 7.1.2.1.3-1: Automation performed by an automated ACM client

The following applies:

- The automated ACM client is enabled/logged-in and connected to ACM server

- The automated ACM client audits and verifies the request to decide whether to apply the configurations or not.

- The automated ACM client takes whatever actions are needed to apply the configurations to the partner MC system. The actions within the partner MC system to apply the configurations are outside the scope of the 3GPP specification

- The MC system provides the possibility for the authorized users to update the automation rules, or to terminate the automated ACM client and accordingly the process automation, if required.

- The partner ACM server provides tracking mechanism for the authorized users in the partner MC system for all automatically performed actions by an automated client.

#### 7.1.2.2 Solution evaluation

This solution provides description for handling stored ACM requests and sending the responses automatically from partner MC systems.

## 7.2 Mapping of solutions to key issues

Table 7.2-1 Mapping of solutions to key issues

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | KI #1 | KI #2 | KI #3 | KI #4 | KI#5 | KI#6 |
| Sol #1 | X |  |  |  |  |  |
| Sol #2 | X |  |  |  |  |  |
| Sol #3 |  |  |  |  |  | X |
| Sol #4 |  |  |  | X |  |  |
| Sol #5 |  |  | X |  |  |  |
| Sol #6 |  |  | X |  |  |  |
| Sol #7 |  |  | X |  | X |  |
| Sol#8 |  |  |  |  | X |  |
| Sol #9 |  |  |  | X |  |  |

## 7.3 Solution #1: Functional architecture

### 7.3.1 Solution description

#### 7.3.1.1 General

This solution addresses key issue 1 defined in clause 5.1.

To allow required exchange of configuration data with a partner MC system, an ACM server and ACM client are added to the functional model of the MC system. This solution uses the interconnection interface and reference points as specified in TS 23.280 [5] for the transfer of administrative configuration information between two MC systems.

#### 7.3.1.2 Functional model

Figure 7.3.1.2-1 illustrates the generic functional model for Administrative Configuration Management eXchange (ACMX).



Figure

An authorized user/administrator as described in 3GPP TS 23.280 [5] in clause 8.1.2 has granted special privileges and is able to use ACMC to communicate with the ACMS in the primary MC system to perform an administrative configuration exchange with a partner MC system.

The ACMS controls the administrative configuration exchange with partner MC system(s) and manages at the same time the interaction with the relevant MC service server entities within the primary MC system.

#### 7.3.1.3 Functional entities description

The Administrative Configuration Management Server (ACMS) is an MC system entity that provides the necessary functionalities to control and perform required transactions to exchange administrative configurations and/or information between partner MC system(s). ACMS has the following functions:

- Supports requests from the ACMC that result in exchanges with the partner MC system to share administrative configurations and information.

- Controls, processes, validates, accepts, forwards or rejects administrative configuration exchange based on a set of pre-defined rules and policies.

The Administrative Configuration Management Client (ACMC) is a functional entity that acts as user client that controls and performs required transactions of administrative configurations and/or information exchange with an Administrative Configuration Management Server.

### 7.3.2 Solution evaluation

This solution provides a generic ACMX functional model allowing the exchange of configuration data between MC systems. It defines for this purpose the new entities ACM server and ACM client to be used in both primary and partner MC systems.

## 7.4 Solution #2: Enhancement to the MC service functional architecture

### 7.4.1 Solution description

This solution builds upon what is already contained in TS 23.280 functional model for the MC services architecture.

### 7.4.2 Functional model description

### 7.4.3 On-network functional model

Each MC service can be represented by an application plane functional model. The functional model across MC services may be similar but is described by the individual functional entities and reference points that belong to that MC service. Within the application plane for an MC service there is a common set of functions and reference points. The common set is shared across services. This common set of functions and reference points is known as the common services core.

Figure 7.4.3.1-1 shows the functional model for the application plane for an MC system.



Figure 7.4.3.1-1: Functional model for application plane for an MC system

The common services core functions and reference points are described in TS 23.280. The new common services core functions and interfaces are described below.

In the model shown in figure 7.4.3.1-1, the following apply:

- The administrative configuration management client is an integrated functional entity of the configuration management client. The administrative configuration management client is described below.

- The administrative configuration management server is an integrated functional entity of the configuration management server. The administrative configuration management server is described below.

### 7.4.4 Administrative configuration management client

The administrative configuration management (ACM) client functional entity acts as the application user agent for an authorized user that is responsible for requesting, approving, and applying configurations between a primary MC system and partner MC system. These configurations include MC service user profile, group management configuration, and associated system parameters. The administrative configuration management client interacts with the administrative configuration management server.

The administrative configuration management client functional entity is supported by the signalling user agent and by the HTTP client functional entities of the signalling control plane.

### 7.4.5 Administrative configuration management server

The administrative configuration management (ACM) server functional entity provides the temporary storage of configuration changes when requests are received from a partner MC system. These configuration changes include MC service user profile, group management configuration, and associated system parameters. The administrative configuration management server validates requests from the administrative configuration management (ACM) client. The ACM client in the partner system is responsible for applying any changes in the MC system once the configurations changes have been validated and approved.

The administrative configuration management server functional entity is supported by the SIP AS and by the HTTP server functional entities of the signalling control plane.

### 7.4.6 Administrative configuration management server and client in a primary MC system and partner MC system

The diagram in Figure 7.4.6-1-1 shows how an administrative configuration management client in the primary MC system communicates with and administrative configuration management client in a partner MC system.



Figure 7.4.6.1-1: Administrative configuration management between a primary and partner MC system

### 7.4.7 Solution evaluation

This solution provides an enhancement to the existing functional architecture to allow for the administrative configuration exchange between interconnected MC systems by re-using existing communications constructs for interfaces and functional entities.

## 7.5 Solution #3: ACMC authorisation

### 7.5.1 Solution description

#### 7.5.1.1 Overview

This solution addresses key issue 6 defined in clause 5.6. It describes the general authorisation concept, triggered by an authorised user via ACMC to enable performing administrative configuration management exchange (ACMX) with partner MC system(s).

An authorised user (i.e. administrator) has the required privileges to use the ACM client to communicate with the primary ACM server for performing an ACMX with a partner MC system(s). The ACM server is in charge of control, process, validate, accept, forward or reject administrative configuration exchange based on a set of pre-defined rules and policies. The primary and the partner ACM servers authorise the exchange between their MC systems.

NOTE: Security aspects including specification of the authorisation procedures are to be decided in SA3.

#### 7.5.1.1a User profile configurations for using ACMX

Table 7.5.1.1a-1 describes the necessary ACM configuration data in the MC service user profile to enable an authorised user to perform ACM transactions with a partner MC system. Configuration and download of the MC service user profile data, which is used by the ACM client and the ACM server, is defined in TS 23.280[5].

Table 7.5.1.1a-1: MC service user profile configurations for authorisation of ACMX (on-network)

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Parameter description** | **ACMC** | **ACMS** |
| Subclause 5.16.4 of 3GPP TS 22.280 [2] | Authorised to perform ACM transactions | Y | Y |
| Subclause 5.16.4 of 3GPP TS 22.280 [2] | List of partner MC systems for which user is authorised to perform ACM transactions (NOTE) |  |  |
|  | > Identity of partner MCPTT system | Y | Y |
| NOTE: Connectivity between ACM servers in a primary MC system and a partner MC system can be defined using existing mechanism as described in Solution #2 of this document. | | | |

NOTE: ACMX can only be performed while on-network.

#### 7.5.1.2 ACMX authorisation for an authorised user

Figure 7.5.1.2-1 describes high level user authorisation flow.

Pre-conditions:

- The primary and partner ACM servers validate the exchange between the MC systems (i.e. by out of band sharing of signing certificate);

NOTE 1: A similar procedure is defined in 3GPP TS 33.180 [4] in clause 5.1.4.2,

- The ACM client can communicate and is authorised to access the ACM server at the primary MC system



Figure 7.5.1.2-1: ACMX authorisation for an authorised user (ACMC)

Procedure:

1. The ACMC of an authorised user requires authorisation from primary ACMS, prior to any exchange with the partner MC system.

NOTE 2: The ACM server will check whether the user of the ACM client is authorised at each transaction.

2. Upon successful authorisation check, the ACMC can start the ACMX session,

3. The partner ACMS verifies the received ACMX requests to decide whether to continue the process.

### 7.5.2 Solution evaluation

This solution provides the authorisation mechanism to control and to enable an authorised user to perform administrative configurations exchange with one or more MC partner systems. The authorisation check of an ACMC is performed by the primary ACMS for each transaction. The primary ACMS is responsible to perform the exchange with the ACMS in the partner MC system.

## 7.6 Solution #4: Group configuration change

### 7.6.1 Solution description

#### 7.6.1.1 General

This solution addresses the following aspects:

- Key issue 4 - change group configuration

- The second precondition in 3GPP TS 23.280, clause 10.2.7.2:

- One or more MC service group members are defined in the partner MC system.

#### 7.6.1.2 Procedure

##### 7.6.1.2.1 Group membership update by authorized user from a partner MC system

The procedure for an authorized MC service user in a partner MC system to request the primary MC system of the MC service group to modify group membership to an interconnection group is shown in figure 7.6.1.2.1-1.

Pre-conditions

- MC system A and MC system B are interconnected

- MC system A and MC system B have implemented an ACMS

- MC system B is the primary MC system of an interconnection group

- The authorized MC service user of MC system A (the partner MC system) wants to modify the membership of MC users of system A in the interconnection group for which MC system B is the primary MC system.

- When a functional alias is used as the target of the request by an ACM client in the MC system A, it is required that the ACM server of MC system A has subscribed to the MC service functional alias controlling server within the MC system A, and that the ACM server of MC system B has subscribed to the MC service functional alias controlling server within the MC system B.



Figure 7.6.1.2.1-1: Group membership update by authorized user from a partner MC system

1. The ACM client in MC system A sends a group membership update request to the ACM server in MC system A, requesting to modify the membership of users from MC system A in an interconnection group for which MC system B is the primary MC system.

2. The ACM server of system A checks whether the MC service user at ACM client A is authorized for the request.

3. The ACM server of MC system A sends the group membership update request to the ACM server of MC system B, the primary MC system of the interconnection group.

4. The ACMS of MC system B sends a process indication to MC system A, and stores, verifies and assesses the incoming request.

4a. Based on local policy, the ACMS of system B may automatically handle the request as described in clause 7.1.2 and send a response to the ACMS of MC system A (i.e. perform step 8).

4b. Otherwise, the ACM server requests verification by an ACM client, following the pending request procedure in clause 7.1.1 if the user is not logged on, and steps 5, 6 and 7. If the request targets a functional alias the ACM server resolves the functional alias (based on the current state of the functional alias) and proceeds as follows:

- if the functional alias is active for one ACM client, the request is sent to the ACM client;

- if the functional alias is active for more than one ACM client, the ACM server sends the request to one of these ACM clients based on the local policy;

- if the functional alias is not currently active, the ACM server stores the request.

5. The ACM server of MC system B sends the stored group membership update request to the ACM client of MC system B.

6. The authorized MC service user of MC system B (manually) screens the content of the group membership update request and decides to approve it or not. The authorized user in the MC system B takes whatever actions are needed to apply the group membership update. The actions within the MC system B to apply this configurations are outside the scope of the 3GPP specifications.

7. The ACM client of MC system B sends a group membership update response to the ACM server of MC system B.

8. The ACM server of MC system B sends the group membership update response to the ACM server of MC system A.

9. The ACM server of MC system A stores the group membership update response. If the ACMC of MC system A is not logged on the ACMS of MC system A will follow the pending request procedure as described in clause 7.1.1.

10. The ACM server of MC system A sends the group membership update response to the ACM client of MC system A.

### 7.6.2 Solution evaluation

This solution introduces a procedure for group membership updates by an authorized user from a partner MC system.

## 7.7 Solution #5: Request to add users for migration to a partner MC system

### 7.7.1 Solution description

#### 7.7.1.1 General

This solution addresses the following aspects:

- Key issue 3 - change user configuration

#### 7.7.1.2 Information flows

##### 7.7.1.2.1 User configuration request

Table 7.7.1.2.1-1 describes the information flow of the user configuration request sent from the primary ACMC to the partner ACMS(s) and, if required, the relevant partner ACMC(s).

Table 7.7.1.2.1-1: User configuration request

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MC service ID | M | The identity of the MC service user at the primary MC system who triggers the information update. |
| Functional alias | O | The functional alias of the MC service user at the primary MC system who triggers the information update. |
| MC service ID | O  (see NOTE 1) | The identity of the MC service user at the partner MC system towards which the information update is sent |
| Functional alias | O  (see NOTE 1) | The functional alias of the MC service user at the partner MC system towards which the information update is sent |
| MC service ID list | M | Set of identities of the migrating MC service user(s). |
| Request category | O | A set of request notification identifiers, e.g. high, medium, low for alerting partner MC system of specific urgencies. |
| Request duration | O | A set of time and date information for each MC service user to inform the partner MC system when the user is expected to attain service at the partner MC system and for how long that MC service user is expected to receive service(s). |
| Additional Information (see NOTE 2) | O | Additional set of MC service user or UE identification information, such as labels, hardware UE identifiers or other identifying information, which may include device descriptions and user capability information. This information is linked to a particular MC service user and/or UE. |
| NOTE 1: Either the MC service ID or the functional alias must be present.  NOTE 2: Further details on what elements need to be included in this message are FFS | | |

##### 7.7.1.2.2 User configuration response

Table 7.7.1.2.2-1 describes the information flow of the user configuration response sent from a primary ACMS to a primary ACMC or a partner ACMC to a partner ACMS and primary ACMS, ACMC.

Table 7.7.1.2.2-1: User configuration response

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| MC service ID | M | The identity of the MC service user at the partner MC system which handled the received update. |
| Functional alias | O | The functional alias of the MC service user at the partner MC system which handled the received update. |
| MC service ID list | M | Set of MC service IDs used in the primary MC system of the migrating MC service user(s) |
| MC service ID list (see NOTE) | M | Set of MC service IDs of the migrating MC service user(s) created by the partner MC system of the migrating MC service user, corresponding to the MC service IDs above. |
| MC service user profile | M | Set of MC service user profiles that corresponds to each MC service ID in the list above.  The user profile contains the initial UE configuration to access the partner MC system as defined in table A.6-1 of 3GPP TS 23.280 [5], and limited information for migration for each MC service user. |
| Response | M | Result information of the user configuration request. When sent within the primary MC system, this IE contains the result of the authorization check. |
| NOTE: The primary MC system of the migrated MC service user keeps a mapping of the MC service IDs used by MC service user(s) in the partner MC system(s). | | |

#### 7.7.1.3 Procedure

The procedure for an authorized MC service user in a primary MC system to request a partner MC system to authorize a list of MC user IDs from its MC System to migrate to that partner MC System is shown in figure 7.7.1.3-1.

Pre-conditions

- The primary and partner MC system(s) are configured to accept connections from relevant ACMCs via the respective ACMSs in each of the connected MC service system(s) and have been configured and authorized successfully to allow exchange of administrative configuration information

- The relevant ACMC(s) and ACMS connection authorizations have been established successfully

- The primary ACMC(s) have access to the MC service user database in the primary MC system – not shown in the procedure below for simplicity reasons

- When a functional alias is used as the target of the request by an ACM client in the primary MC system, it is required that the primary ACM server has subscribed to the MC service functional alias controlling server within the primary MC system, and that the partner ACM server has subscribed to the MC service functional alias controlling server within the partner MC system.



Figure 7.7.1.3-1: User configuration request in partner MC system

1. The primary ACMC sends user configuration request to the primary ACMS, requesting to authorize a list of MC users from the primary MC System to migrate to the partner MC System.

2. The primary ACMS performs an authorization check to verify that the MC service user is authorized to perform this action. A successful authorization check results in the user configuration request being forwarded to the relevant partner ACMS.

3. The primary ACMS sends the user configuration request to the partner ACMS.

NOTE 1: Step 3 is not followed if the authorization was unsuccessful.

4. The partner ACMS sends a process indication to the primary MC system, and stores, verifies and assesses the incoming request.

4a. Based on local policy, the partner ACMS may automatically handle the request as described in clause 7.1.2 and send a response to the primary ACMS (i.e. perform step 8).

4b. Otherwise, the ACM server requests verification by an ACM client, following the pending request procedure in clause 7.1.1 if the user is not logged on, and steps 5, 6 and 7. If the request targets a functional alias the ACM server resolves the functional alias (based on the current state of the functional alias) and proceeds as follows:

- if the functional alias is active for one ACM client, the request is sent to the ACM client;

- if the functional alias is active for more than one ACM client, the ACM server sends the request to one of these ACM clients based on the local policy;

- if the functional alias is not currently active, the ACM server stores the request.

5. The partner ACMS sends the stored user configuration request to the partner ACMC.

6. The authorized MC service user of partner MC system checks the content of the user configuration request and decides whether to approve it or not. The authorized user in the partner MC system takes whatever actions are needed to apply the configurations. The actions within the partner MC system to apply the configurations are outside the scope of the 3GPP specifications.

7. The partner ACMC sends user configuration response to the partner ACMS.

8. The partner ACMS sends user configuration response to the primary ACMS.

9. The primary ACMS stores the user configuration response. If the primary ACMC is not logged on the primary ACMS will follow the pending request procedure as described in clause 7.1.1.

10. The primary ACM S sends the user configuration response to the primary ACMC.

### 7.7.2 Solution evaluation

This solution introduces a solution to request to add users for migration to a partner MC system. The solution returns to the primary system the status of the request, and all necessary information that is needed in the primary MC system to configure the migrating users.

## 7.8 Solution #6: Request to remove users for migration from a partner MC system

### 7.8.1 Solution description

7.8.1.1 General

This solution addresses the following aspects of Key issue 3 – Change user configuration.

When certain users no longer are needed for migration to a partner system, there should be a means for an authorized user in the primary MC system to request that certain users be removed from migration access in the partner MC system. This maintenance activity is necessary, as once users are added for migration, it cannot be assumed that their migration access will be indefinite.

#### 7.8.1.2 Information flows

##### 7.8.1.2.1 Remove user configuration request

Table 7.8.1.2.1-1 describes the information flow of the remove user configuration request sent from a primary MC system ACM client to a partner MC system ACM client.

Table 7.8.1.2.1-1: Remove user configuration request

|  |  |  |
| --- | --- | --- |
| **Information element** | **Status** | **Description** |
| MC service ID | M | The identity of the authorized user in the primary MC system who is sending the remove user configuration request. |
| Functional alias | O | The functional alias of the MC service user at the primary MC system who triggers the Group information provision request. |
| MC service ID | O (see NOTE) | The identity of the authorized user in the partner MC system that is the target of the request. |
| Functional alias | O (see NOTE) | The functional alias of the MC service user at the partner MC system towards which the Group information provision request is sent |
| MC service ID list | M | The list of users in the partner MC system that are being requested to be removed for migration. |
| Additional information list | O | Additional information describing the reason for removing each requested user in the list for migration from the primary MC system to the partner MC system. |
| NOTE: Either the MC service ID or the functional alias must be present. | | |

##### 7.8.1.2.2 Remove user configuration response

Table 7.8.1.2.2-1 describes the information flow of the remove user configuration response sent from from a partner MC system ACM client to a primary MC system ACM client.

Table 7.8.1.2.2-1: Remove user configuration response

|  |  |  |
| --- | --- | --- |
| **Information element** | **Status** | **Description** |
| MC service ID | M | The identity of the authorized user in the partner MC system who is sending the remove user configuration response. |
| Functional alias | O | The functional alias of the MC service user at the partner MC system who is sending the remove user configuration response. |
| MC service ID | O (see NOTE) | The identity of the authorized user in the primary MC system that is the target of the response. |
| Functional alias | O (see NOTE) | The functional alias of the MC service user in the primary MC system that is the target of the response. |
| MC service ID list | M | The list of users in the partner MC system that were requested to be removed for migration. |
| Response | M | Result information for each user in the list for removal. Success or fail. |
| Reason | O | Additional information that explains the response for each user in the list. |
| NOTE: Either the MC service ID or the functional alias must be present | | |

#### 7.8.1.3 Remove user configuration request from a partner MC system

The procedure for an authorized MC service user in the primary MC system, that is sent to an authorized user in the partner MC system, to request that certain users be removed from migration access in the partner MC system is shown in figure 7.8.1.3-1.

Pre-conditions

- The primary MC system and the partner MC system are interconnected.

- The MC service user in the primary MC system is authorized to request a list of MC service users be removed from the partner MC system for migration from the primary MC system.

- At the start of the procedure the target authorized user in the partner MC System is logged on.

- The users that are targetted to be removed by this procedure are no longer migrated to the partner MC system. The need for these users to migrate to the partner MC system no longer exists.

- When a functional alias is used as the target of the request by an ACM client in the primary MC system, it is required that the primary ACM server has subscribed to the MC service functional alias controlling server within the primary MC system, and that the partner ACM server has subscribed to the MC service functional alias controlling server within the partner MC system.



Figure 7.8.1.3-1: Remove user configuration request from a partner MC system

1. The ACM client in the primary MC system sends a remove user configuration request to the ACM server in the primary MC system. This request includes a list of MC service users to be removed for migration access in the partner MC system.

2. The ACM server in the primary MC system validates whether the MC service user is authorized for the request.

3. The ACM server in the primary MC system sends the remove user configuration request to the ACM server in the partner MC system.

4. The partner ACMS sends a process indication to the primary MC system, and stores, verifies and assesses the incoming request.

4a. Based on local policy, the partner ACMS may automatically handle the request as described in clause 7.1.2 and send a response to the primary ACMS (i.e. perform step 8).

4b. Otherwise, the ACM server requests verification by an ACM client, following the pending request procedure in clause 7.1.1 if the user is not logged on, and steps 5, 6 and 7. If the request targets a functional alias the ACM server resolves the functional alias (based on the current state of the functional alias) and proceeds as follows:

- if the functional alias is active for one ACM client, the request is sent to the ACM client;

- if the functional alias is active for more than one ACM client, the ACM server sends the request to one of these ACM clients based on the local policy;

- if the functional alias is not currently active, the ACM server stores the request.

5. The ACM server in the partner MC System sends the remove user configuration request to the ACM client in the partner MC system.

6. The authorized MC service user of partner MC system checks the content of the request and decides whether to approve it or not. The authorized MC service user in the partner MC system takes whatever actions are needed to remove the requested user from migration access to the partner MC system from the primary MC system. The actions within the partner MC system to remove users are outside the scope of the 3GPP specifications.

7. The ACM client of the partner MC system sends a remove user configuration response to the ACM server in the partner MC system. The target of this response is the original MC service user in the primary MC system that sent the remove user configuration request.

8. The ACM server in the partner MC system sends the remove user configuration response to the ACM server in the primary MC system.

9. The ACM server in the primary MC system stores the remove user configuration response. If the primary ACMC is not logged on the primary ACMS will follow the pending request procedure as described in clause 7.1.1.

10. The ACM server in the primary MC system sends the remove user configuration response to the ACM client in the primary MC system.

11. The authorized MC service user in the primary MC system takes whatever actions are needed (if any) to update the user profiles in the primary MC system for those users that no longer have migration access to the partner MC system.

### 7.8.2 Solution evaluation

This solution provides a means for an authorized user in the primary MC system to request that certain users be removed from migration access in the partner MC system. Such a solution is needed because once users are added for migration, it cannot be assumed that their migration access to the partner MC system will be indefinite.

## 7.9 Solution #7: Update MC service UE initial configuration

### 7.9.1 Solution description

#### 7.9.1.1 General

This solution addresses the following aspects:

- Key issue 3 - change user configuration

- Key issue 5 – Service configuration data

This solution enables an authorized user to provide configuration data to a partner MC system needed to update the initial MC service UE configuration data to be stored in an MC service UE enabling migration to a partner MC system. The initial MC service configuration is a pre-condition for authentication and authorization for MC services in a partner MC system.

Initial MC service UE configuration data can be exchanged between the MC systems using ACMX entities as described in the following procedure. This solution allows to keep a partner MC system up to date with regard to the required initial MC service UE configuration date needed for migration.

#### 7.9.1.2 Information flows

##### 7.9.1.2.1 Update MC service UE initial configuration

Table 7.9.1.2.1-1 describes the information flow from the primary ACMC to the primary ACMS, and from the primary ACMS to the partner ACMS, for updating initial MC service UE configuration data information that is required by the partner MC system for preparing migrating MC service UEs.

Table 7.9.1.2.1-1: Update MC service UE initial configuration

|  |  |  |
| --- | --- | --- |
| **Information element** | **Status** | **Description** |
| MC service ID | M | The identity of the MC service user at the primary MC system who triggers the information update. |
| Functional alias | O | The functional alias of the MC service user at the primary MC system who triggers the information update. |
| MC service ID | O  (see NOTE 1) | The identity of the MC service user at the partner MC system towards which the information update is sent |
| Functional alias | O  (see NOTE 1) | The functional alias of the MC service user at the partner MC system towards which the information update is sent |
| MC service ID list | M | Set of MC service IDs of the migrating MC service users that belong to the primary MC system. |
| MC service UE initial configuration data (see NOTE 2) | M | This information element contains the information as specified in table A.6-1 of 3GPP TS 23.280 [5] corresponding to the MC service IDs above. |
| NOTE 1: Either the MC service ID or the functional alias must be present.  NOTE 2: The MC service UE label defined in TS 23.280 [5], Annex 6 is sent in this information element only in case the request is targeting a certain MC service UE(s), otherwise this information is not present. | | |

##### 7.9.1.2.2 Update MC service UE initial configuration response

Table 7.9.1.2.2-1 describes the information flow from the partner ACMC to the partner ACMS and from partner ACMS to primary ACMS.

Table 7.9.1.2.2-1: Update MC service UE initial configuration response

|  |  |  |
| --- | --- | --- |
| **Information element** | **Status** | **Description** |
| MC service ID | M | The identity of the MC service user at the partner MC system which handled the received update. |
| Functional alias | O | The functional alias of the MC service user at the partner MC system which handled the received update. |
| Result | M | Result information of the update MC service UE initial configuration. |

#### 7.9.1.3 Procedure

The procedure for an authorized MC service user in a primary MC system to update the partner MC system with the initial MC service UE configuration data information is shown in figure 7.9.1.3-1.

Pre-conditions

- The primary and partner MC system(s) are configured to accept connections from relevant ACMCs via the respective ACMSs in each of the connected MC service system(s) and have been configured and authorized successfully to allow exchange of administrative configuration information

- The relevant ACMC(s) and ACMS connection authorizations have been established successfully

- The set of MC service IDs and the MC service UE initial configuration of the migrating MC service users have been already sent by the primary MC system to the partner MC system, as specified in solution #5.

- When a functional alias is used as the target of the request by an ACM client in the primary MC system, it is required that the primary ACM server has subscribed to the MC service functional alias controlling server within the primary MC system, and that the partner ACM server has subscribed to the MC service functional alias controlling server within the partner MC system.



Figure 7.9.1.3-1: Update MC service UE initial configuration

1. The primary ACMC sends an update MC service UE initial configuration to the primary ACMS, providing the initial MC service UE configuration data as specified in 3GPP TS 23.280 [5], Annex 6 to the primary MC System.

2. The primary ACMS performs an authorization check to verify that the MC service user is authorized to perform this action. A successful authorization check results in the Update MC service UE initial configuration being forwarded to the relevant partner ACMS. If the authorization check is failed the next steps are not followed

3. The primary ACMS sends the update MC service UE initial configuration to the partner ACMS.

4. The partner ACMS processes the incoming update. Based on local policy, the partner ACMS may automatically handle the request and send an update MC service UE initial configuration response to the primary ACMS. Otherwise the ACM server should request verification by an ACM client.

If the request targets a functional alias the ACM server resolves the functional alias (based on the current state of the functional alias) and proceeds as follows:

- if the functional alias is active for one ACM client, the request is sent to the ACM client;

- if the functional alias is active for more than one ACM client, the ACM server sends the request to one of these ACM clients based on the local policy;

- if the functional alias is not currently active, the ACM server stores the request.

5. The partner ACMS may send a process pending indication to the primary MC system.

NOTE 1: There may be a considerable pause between step 4 and 7.

6. The partner ACMS forwards the stored update MC service UE initial configuration to the partner ACMC.

7. The authorized MC service user of partner MC system processes the received update MC service UE initial configuration.

NOTE 2: It is out of the scope of this document how the received initial MC service UE configuration data is applied to MC service UEs (before migration).

8. The partner ACMC sends update MC service UE initial configuration response to the partner ACMS.

9. The partner ACMS sends update MC service UE initial configuration response to the primary ACMS.

10. The primary ACMC stores the update MC service UE initial configuration response.

NOTE 3:There may be a considerable pause between step 10 and 11.

11. The primary ACMS forwards the update MC service UE initial configuration response to the primary ACMC.

### 7.9.2 Solution evaluation

This solution enables an authorized user of the primary MC system to provide an update of the MC service UE initial configuration to be stored in the MC service user profiles in a partner system, enabling migration to the primary MC system. The solution addresses key issue 3 and key issue 5.

## 7.10 Solution #8: MC service user profile update request while receiving MC service from a partner MC system

### 7.10.1 Solution description

#### 7.10.1.1 General

This solution addresses the following aspects:

- Key issue 5 – Service configuration data

For an MC service user, when migrating and receiving MC service from a partner MC system, it will use the user profile resulted from profile exchange between the primary and partner MC systems as specified in 3GPP TS 23.280, clause 10.1.4.3.2. This solution enables an authorized user in primary MC system to request changes to MC service user profile, while these user(s) are migrated to a partner MC system.

The update of MC service user profile can be done between the MC systems using ACMX entities as described in the following procedure.

#### 7.10.1.2 Information flows

##### 7.10.1.2.1 MC service user profile update request

Table 7.10.1.2.1-1 describes the information flow from the primary ACMC to the primary ACMS, and from the primary ACMS to the partner ACMS.

Table 7.10.1.2.1-1: MC service user profile update request

|  |  |  |
| --- | --- | --- |
| **Information element** | **Status** | **Description** |
| MC service ID | M | The identity of the MC service user at the primary MC system who triggers the request. |
| Functional alias | O | The functional alias of the MC service user at the primary MC system triggers request. |
| MC service ID | O (see NOTE) | The identity of the MC service user at the partner MC system towards which the request is sent |
| Functional alias | O (see NOTE) | The functional alias of the MC service user at the partner MC system towards which the request is sent |
| MC service ID | M | MC service ID of the migrated MC service user, which has been created by the partner MC system. |
| MC service user profile | M | The suggested updated MC service user profile on the partner MC system. |
| Additional Information | O | Additional information regarding the suggested updated MC service user profile on the partner MC system. |
| NOTE: Either the MC service ID or the functional alias must be present. | | |

##### 7.10.1.2.2 MC service user profile update response

Table 7.10.1.2.2-1 describes the information flow from the partner ACMC to the partner ACMS and from partner ACMS to primary ACMS.

Table 7.10.1.2.2-1: MC service user profile update response

|  |  |  |
| --- | --- | --- |
| **Information element** | **Status** | **Description** |
| MC service ID | M | The identity of the MC service user at the partner MC system which handled the received request. |
| Functional alias | O | The functional alias of the MC service user at the partner MC system which handled the received request. |
| MC service ID | M | MC service ID of the migrated MC service user. |
| Result | M | Result information of the MC service user profile update request, |

#### 7.10.1.3 Procedure

The procedure for an authorized MC service user in a primary MC system to request MC service user profile update from a partner MC system is shown in figure 7.10.1.3-1.

Pre-conditions

- The primary and partner MC system(s) are configured to accept connections from relevant ACMCs via the respective ACMSs in each of the connected MC service system(s) and have been configured and authorized successfully to allow exchange of administrative configuration information

- The relevant ACMC(s) and ACMS connection authorizations have been established successfully

- The authorized user at the primary MC system needs to update the MC service user profile, for an MC service user already migrated and receiving services in a partner MC system.

- When a functional alias is used as the target of the request by an ACM client in the primary MC system, it is required that the primary ACM server has subscribed to the MC service functional alias controlling server within the primary MC system, and that the partner ACM server has subscribed to the MC service functional alias controlling server within the partner MC system.



Figure 7.10.1.3-1: MC service user profile update

1. The primary ACMC sends MC service user profile update request to the primary ACMS providing the required changes for the MC service user that is migrated to the partner MC System.

2. The primary ACMS performs an authorization check to verify that the MC service user is authorized to perform this action. A successful authorization check results in the MC user profile update request being forwarded to the relevant partner ACMS. If the authorization was unsuccessful, step 3 is not followed and the procedure is stopped.

3. The primary ACMS sends the MC service user profile update request to the partner ACMS.

4. The partner ACMS sends a process indication to the primary MC system, and stores, verifies and assesses the incoming request.

4a. Based on local policy, the partner ACMS may automatically handle the request as described in clause 7.1.2 and send a response to the primary ACMS (i.e. perform step 8).

4b. Otherwise, the ACM server requests verification by an ACM client, following the pending request procedure in clause 7.1.1 if the user is not logged on, and steps 5, 6 and 7. If the request targets a functional alias the ACM server resolves the functional alias (based on the current state of the functional alias) and proceeds as follows:

- if the functional alias is active for one ACM client, the request is sent to the ACM client;

- if the functional alias is active for more than one ACM client, the ACM server sends the request to one of these ACM clients based on the local policy;

- if the functional alias is not currently active, the ACM server stores the request.

5. The partner ACMS forwards the stored MC service user profile update request to the partner ACMC.

6. The authorized MC service user of partner MC system checks the content of the MC service user profile update request and decides whether to approve it or not. The authorized user in the partner MC system takes whatever actions are needed to apply the MC service user profile update. The actions within the partner MC system to apply this configuration are outside the scope of the 3GPP specifications.

7. The partner ACMC sends MC service user profile update response to the partner ACMS.

8. The partner ACMS sends MC service user profile update response to the primary ACMS.

9. The primary ACMS stores the MC service user profile update response. If the primary ACMC is not logged on the primary ACMS will follow the pending request procedure as described in clause 7.1.1.

10. The primary ACMS forwards the MC service user profile update response to the primary ACMC.

### 7.10.2 Solution evaluation

This solution enables an authorized user in the primary MC system to request an update to the MC service user profile while the MC user is migrated and served by the partner MC system. This solution addresses key issue 5.

## 7.11 Solution #9: Provide Interconnection Group IDs

### 7.11.1 Solution description

#### 7.11.1.1 General

This solution addresses the following aspects:

- Key issue 4 – Group configuration data

“The MC service group is configured in the MC service user profiles … “

This solutions enables an authorized user to provide a list of interconnection group ID(s) to a selected authorized user of a partner MC system.

#### 7.11.1.2 Information flows

##### 7.11.1.2.1 Group information provision request

Table 7.11.1.2.1-1 describes the information flow of the Group information provision request sent from the primary ACMC to the partner ACMS(s) and partner ACMC(s).

Table 7.11.1.2.1-1: Group information provision request

|  |  |  |
| --- | --- | --- |
| **Information element** | **Status** | **Description** |
| MC service ID | M | The identity of the MC service user at the primary MC system who triggers the Group information provision request. |
| Functional alias | O | The functional alias of the MC service user at the primary MC system who triggers the Group information provision request. |
| MC service ID | O (see NOTE) | The identity of the MC service user at the partner MC system towards which the Group information provision request is sent |
| Functional alias | O (see NOTE) | The functional alias of the MC service user at the partner MC system towards which the Group information provision request is sent |
| MC service group ID list | M | A list of one or more MC service group IDs |
| Group description per MC service group ID | O | A text description indicating the intended operational use for every MC service group ID in the list |
| NOTE: Either the MC service ID or the functional alias must be present. | | |

##### 7.11.1.2.2 Group information provision response

Table 7.11.1.2.2-1 describes the information flow of the Group information provision response from a partner ACMC to a partner ACMS, the primary ACMS and the primary ACMC.

Table 7.11.1.2.2-1: Group information provision response

|  |  |  |
| --- | --- | --- |
| **Information element** | **Status** | **Description** |
| MC service ID | M | The identity of the MC service user at the partner MC system who generates the Group information provision response. |
| Functional alias | O | The functional alias of the MC service user at the partner MC system who generates the Group information provision response. |
| Provision status | M | Indicates the provisioning result |

#### 7.11.1.3 Procedure

##### 7.11.1.3.1 Authorized user providing interconnection group ID(s) to authorized user of a partner MC system

The procedure, which enables an authorized MC service user of a primary MC system to provide a list of interconnection group ID(s) to a selected authorized user of a partner MC system, is shown in figure 7.11.1.3.1-1.

Pre-conditions

- primary MC system and partner MC system are interconnected

- both MC systems have implemented an ACMS functionality

- the primary MC system is the MC service group home system for one or more interconnection groups

- The MC service user of the primary MC system is authorized to provide a list of interconnection group IDs to a selected authorized user of the partner MC system .

- When a functional alias is used as the target of the request by an ACM client in the primary MC system, it is required that the primary ACM server has subscribed to the MC service functional alias controlling server within the primary MC system, and that the partner ACM server has subscribed to the MC service functional alias controlling server within the partner MC system.



Figure 7.11.1.3.1-1: Group information provision to an authorized user of a partner system

1. The ACM client in the primary MC system sends a group information provision request to the ACM server in the primary MC system, providing a list of interconnection group IDs and the ID of the selected authorized user in the partner MC system.

2. The ACM server of the primary MC system checks whether the MC service user at ACM client is authorized for the request.

3. The ACM server of the primary MC system forwards the group information provision request to the ACM server in the partner MC system.

4. The partner ACMS sends a process indication to the primary MC system, and stores, verifies and assesses the incoming request.

4a. Based on local policy, the partner ACMS may automatically handle the request as described in clause 7.1.2 and send a response to the primary ACMS (i.e. perform step 8).

4b. Otherwise, the ACM server requests verification by an ACM client, following the pending request procedure in clause 7.1.1 if the user is not logged on, and steps 5, 6 and 7. If the request targets a functional alias the ACM server resolves the functional alias (based on the current state of the functional alias) and proceeds as follows:

- if the functional alias is active for one ACM client, the request is sent to the ACM client;

- if the functional alias is active for more than one ACM client, the ACM server sends the request to one of these ACM clients based on the local policy;

- if the functional alias is not currently active, the ACM server stores the request.

5. The ACM server of the partner MC system forwards the stored group information provision request to the ACM client of the partner MC system.

6. The selected authorized user of the partner MC System processes the interconnection group IDs, e.g. by saving the information for future use. The authorized user in the partner MC system takes whatever actions are needed to handle the request. The actions taken within the partner MC system are outside the scope of the 3GPP specifications.

7. The ACM client of the partner MC system sends a group information provision response to the ACM server of the partner MC system.

8. The ACM server of the partner MC system forwards the group information provision response to the ACM server in the primary MC system.

9. The ACM server of the primary MC system stores the group information provision response. If the primary ACMC is not logged on the primary ACMS will follow the pending request procedure as described in clause 7.1.1.

10. The ACM server of the primary MC system forwards the group information provision response to the ACM client of primary MC system, informing the authorized user of the primary MC system that the list of interconnection group IDs has been provided to the selected authorized user of the partner MC system.

### 7.11.2 Solution evaluation

This solution enables an authorized user from a primary MC system to provide interconnection group IDs to a selected authorized user of a partner MC system.

# 8 Evaluation

## 8.1 Overview

All the key issues and solutions specified in this technical report are listed in table 8.1-1. It includes the mapping of the key issues to the solutions and corresponding solution evaluations. In addition, table 8.1-1 lists the impacts to other working groups that will need consideration during the normative phase.

Table 8.1-1: Key issue and solution evaluation

| **Key issues** | **Solution** | **Evaluation**  **(subclause reference)** | **Dependency on other working groups** |
| --- | --- | --- | --- |
| Key issue 1: functional architecture | Solution #1: Functional architecture | 7.3.2 | - |
| Solution #2: Enhancement to the MC service functional architecture | 7.4.7 | - |
| Key issue 2 – Identification | - |  | - |
| Key issue 3 – Change user configuration | Solution #5: Request to add users for migration to a partner MC system | 7.7.2 | - |
| Solution #6: Request to remove users for migration from a partner MC system | 7.8.2 | - |
| Solution #7: Update MC service UE initial configuration | 7.9.2 | - |
| Key issue 4 – Group configuration data | Solution #4: Group configuration change | 7.6.2 | - |
| Solution #9: Provide Interconnection Group IDs | 7.11.2 | - |
| Key issue 5 – Service configuration data | Solution #7: Update MC service UE initial configuration | 7.9.2 | - |
| Solution #8: MC service user profile update request while receiving MC service from a partner MC system | 7.10.2 | - |
| Key issue 6: authorization | Solution #3: ACMC authorization | 7.5.2 | SA3 |
| Key issue 7: Secure exchange and topology hiding | - |  | - |

## 8.2 Overall evaluation of key issue#1

Solution #1 and solution #2 together fulfil the needs of key issue #1.

Solution#1 describes the basic functional model required to support the administrative configuration exchange between MC systems. It introduces the new entities ACM client and ACM server in charge of performing the required actions and describes their functionalities.

Solution #2 provides the new common services core functions for administrative configuration management, as an integrated functional entity of the configuration management client (ACMC), and as an integrated functional entity of the configuration management server (ACMS). It also uses the interconnection interface and reference points as specified in TS 23.280 [5] for the transfer of ACMX between the MC systems.

## 8.3 Overall evaluation of key issue#2

The solutions in this study use the MC service user identities defined and used for common services in an MC system (i.e. MC service ID and functional alias) as specified under clause 8 in 3GPP TS 23.280 [5].

## 8.4 Overall evaluation of key issue#3

Solution #5, solution #6 and solution #7 provide solutions for adding users for migration to a partner MC system, updating the MC service user configuration information and removing certain users from migration access in the partner MC system.

## 8.5 Overall evaluation of key issue#4

Solution #4 and solution #9 provide procedures for exchanging and updating the group configuration information between interconnected MC systems.

## 8.6 Overall evaluation of key issue#5

Solution#7 and solution #8 provide procedures for updating and exchanging service configuration data for an MC service user before, and after the MC user has migrated and is served by the partner MC system.

## 8.7 Overall evaluation of key issue#6

Solution#3 provides the general authorization concept and the necessary configurations to enable performing administrative configuration management exchange between interconnected MC systems.

## 8.8 Overall evaluation of key issue#7

Solution #2 provides an architecture solution that reuses existing interfaces and functional entities that utilize technical security mechanisms that already exist to communicate between the involved MC systems while hiding the network topology.

The procedures in solutions #4 through #9 enable the authorized user in the MC system, where the changes are to be applied, the control to accept or reject the changes before they are applied.

# 9 Conclusions

This technical report fulfils the objective to develop solutions for sharing of administrative configuration between interconnected MC service systems. It identifies enhancements to be included in the technical specifications for MC services and in the common functional architecture.

The results from the study will be considered for follow-up normative work in Rel-19 as follows:

- Definition of terms and abbreviations captured in clause 3 will be reused;

- The common ACM procedures in clause 7.1 will be reused;

- The following key issues (clause 5) and individual solutions (clause 7) are considered to be the candidate solutions with necessary enhancements as appropriate:

- For key issue#1, solution #1 provides an overview of the required functional model for ACM, and solution#2 applies this enhancement to the existing functional model in TS 23.280 [5].

- For key issue#3, solution#5, solution#6 and solution#7.

- For key issue#4, solution#4 and solution#9.

- For key issue#5, solution#7 and solution#8.

- For key issue#6, solution#3.

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-02 | SA6#47-e |  |  |  |  | TR skeleton as approved by SA6 in S6-220085 | 0.0.0 |
| 2022-02 | SA6#47-e |  |  |  |  | S6-220096 | 0.1.0 |
| 2022-04 | SA6#48-e |  |  |  |  | S6-220537, S6-220538, S6-220531, S6-220532, S6-220533, S6-220534, S6-220619, S6-220620 | 0.2.0 |
| 2022-05 | SA6#49-e |  |  |  |  | S6-221009, S6-221059, S6-221061, S6-221062, S6-221374, S6-221375 | 0.3.0 |
| 2022-10 | SA6#51-e |  |  |  |  | S6-223050, S6-223026, S6-222982, S6-222874, S6-223051. | 0.4.0 |
| 2022-11 | SA6#52 |  |  |  |  | S6-223162, S6-223356, S6-223614, S6-223606, S6-223539, S6-223496 | 0.5.0 |
| 2022-12 | SA#98-e | SP-221217 |  |  |  | Submitted to SA#98-e for information | 1.0.0 |
| 2023-01 | SA6#52-bis-e |  |  |  |  | S6-230298 | 1.1.0 |
| 2023-03 | SA6#53 |  |  |  |  | S6-230815, S6-230816, S6-230817, S6-230818, S6-230820, S6-230821, S6-230822, S6-230823, S6-230826, S6-230827, S6-230828. | 1.2.0 |
| 2023-04 | SA6#54-e |  |  |  |  | S6-231125, S6-231126, S6-231127, S6-231128, S6-231129, S6-231131, S6-231132, S6-231469, S6-231553, S6-231602. | 1.3.0 |
| 2023-05 | SA6#55 |  |  |  |  | S6-231694 | 1.4.0 |
| 2023-06 | SA#100 | SP-230689 |  |  |  | Submitted to SA#100 for approval | 2.0.0 |
| 2023-06 | SA#100 | SP-230689 |  |  |  | MCC Editorial update for publication after TSG SA approval (SA#100) | 18.0.0 |