|  |
| --- |
| 3GPP TR 22.881 V18.1.0 (2021-12) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on sharing administrative configuration between interconnected MCX systems(Release 18) |
|   |
|  |  |
|  |
| 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. |

|  |
| --- |
| KeywordsLTE, 5G, MCPTT, MCVideo, MCData |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://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.© 2021, 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 members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

Introduction 4

1 Scope 5

2 References 5

3 Definitions of terms, symbols and abbreviations 5

3.1 Terms 5

3.2 Symbols 5

3.3 Abbreviations 5

4 Overview 5

5 Use cases 6

5.1 Changing group membership in a Partner MCX Service System 6

5.1.1 Description 6

5.1.2 Pre-conditions 6

5.1.3 Service Flows 6

5.1.4 Post-conditions 7

5.1.5 Existing features partly or fully covering the use case functionality 7

5.1.6 Potential New Requirements needed to support the use case 7

5.2 Incident response involving multiple countries 7

5.2.1 Description 7

5.2.2 Pre-conditions 8

5.2.3 Service Flows 8

5.2.4 Post-conditions 9

5.2.5 Existing features partly or fully covering the use case functionality 9

5.2.6 Potential New Requirements needed to support the use case 9

6 Security Aspects 9

6.1 Introduction 9

6.2 Potential requirements 9

7 Additional considerations 10

8 Consolidated Potential Requirements 10

8.1 Changing group membership in a Partner MCX Service System 10

8.2 Incident response involving multiple countries 10

8.3 Security Aspects 11

9 Conclusions and Recommendations 11

Annex <A>: <Title> 12

Annex <B> (informative): Bibliography 13

Annex <X> (informative): Change history 14

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

# Introduction

Editor’s note: Text to be provided.

# 1 Scope

The present document studies use cases that assess under which circumstances interconnected MCX Service Systems exchange administrative and security relevant data and information.

Its objective is to identify new potential requirements related to the use cases and new high-level security requirements related to interconnection of MCX Service Systems and migration of MCX Users and MCX Service Groups.

# 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".

# 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].

## 3.2 Symbols

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

## 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].

# 4 Overview

Considering public safety users specifically, different scenarios of public safety broadband wireless communications systems deployments will emerge, but some requirements remain common. In international or multi agency collaboration scenarios public safety MCX Service Users are required to roam or migrate from one system to another, need to use MCX Services or be included in specific communication events in a Partner MCX Service System on a temporary basis.

Public safety may also deploy their own mobile, local, countrywide or national broadband communications systems. In order to grant visiting MCX Service Users access to a Partner MCX Service System and its services, a mechanism is required which allows the request and/or transmission of administrative configuration data, to be exchanged between connected MCX Service Systems. This type of administrative configuration data is used for adding MCX Service Users into a Partner MCX Service System’s user database and for enabling or disabling certain services. Relevant information can be exchanged prior to the visiting MCX Service Users arriving from a Partner MCX Service System or dynamically during events for example.

Such mechanism can be realised with the administrative configuration data and information exchange concept, discussed in this study.

# 5 Use cases

## 5.1 Changing group membership in a Partner MCX Service System

### 5.1.1 Description

A Dutch police officer currently located in Germany is witnessing a traffic accident involving a Dutch truck. The Dutch MC UE is equipped with a roaming SIM card, is registered in a public German EPS/5GS, which allows the Dutch police officer to use Dutch MCPTT services only and there is no affiliation to German police or emergency services talk groups granted.

In order to offer support to local law enforcement the police officer contacts the Dutch command and control centre in the Dutch MCX Service System and offers assistance at the scene of the accident. The Dutch control centre contacts the German MCX Service System via the High Level Protocol and announces that a police officer with Dutch and German language skills is available at the scene of the accident and requests the ability to participate in the local police incident communications.

The relevant German command and control room receives the support offer and approves the request. The Dutch police officer then receives configuration data and authorisation allowing him to affiliate to the local Police talk group in the German MCX Service System.

The Dutch police officer can now communicate directly with the German police officers on site to support the accident investigation, adding a witness statement.

### 5.1.2 Pre-conditions

1. The Dutch police officer has to have a valid MCX subscription in the Dutch MCX Service System
2. There is an operational agreement between the Dutch and the German Mission Critical Organization and a link has been established between the systems that allows exchange of administrative configuration information
3. An agreement has to be in place that allows the Dutch police officer’s UE to register on a public German EPS/5GS which enables initial communication with the Dutch MCX Service System authorized user(s)

### 5.1.3 Service Flows

1. The Dutch Police officer informs their Dutch MCX Service System’s authorized user(s)
2. The authorized user(s) in the Dutch Police officers Primary MCX Service System analyses the received information and collects additional information, which need to be provided to the Partner MCX Service System
3. The authorized user(s) in the Dutch MCX Service System establishes contact via a separate administrative configuration protocol with the German MCX Service System
4. The Dutch and the German MCX Service Systems exchange the relevant administrative and security information via the separate administrative configuration protocol
5. The relevant authorized user(s) in the German MCX Service System, either automatically or manually, processes the request
6. After acceptance or successful checks/authorisations, the Dutch Police officer’s user profile is updated to include the relevant information, such as user group configuration and encryption key material, assigned by the German MCX Service System
7. The Dutch police officer’s UE affiliates to the German MCX Service Group via the Dutch MCX Service System and its Group communication is routed from the public German EPS/5GS through the Dutch MCX Service System to the German MCX Service System

### 5.1.4 Post-conditions

1. The Dutch Police officer can now select and participate in the relevant German talk group(s)

### 5.1.5 Existing features partly or fully covering the use case functionality

The following requirements refer to 3GPP TS 22.280.

[R-6.17.2-004] An MCX Service shall provide mechanisms to allow an MCX User on the Primary MCX Service System to affiliate and communicate in an MCX Service Group from a Partner MCX Service System, subject to authorization from the Primary MCX Service System and the Partner MCX Service System where the MCX Service Group is defined.

[R-6.17.2-007] End to end security of an MCX Service Group communication (including in Partner MCX Service Systems) shall be based on parameters obtained from the MCX Service system where the MCX Service Group is defined.

### 5.1.6 Potential New Requirements needed to support the use case

[PR 5.1.6.1] An MCX Service shall provide secure mechanisms to allow an authorised MCX User to request MCX User configuration changes in one or more Partner MCX Service Systems.

[PR 5.1.6.2] An MCX Service shall provide secure mechanisms to allow an authorised MCX User to evaluate and respond to requests for configuration changes from Partner MCX Service Systems.

[PR 5.1.6.3] An MCX Service shall provide secure mechanisms to allow an authorised MCX User to configure automatic responses to categories of requests for configuration changes from Partner MCX Service Systems.

## 5.2 Incident response involving multiple countries

### 5.2.1 Description

A train carrying passengers and cargo has derailed in the border region between Belgium, The Netherlands and Germany and collided with a freight train transporting chemicals and other flammable material. Injured persons need to be rescued, derailed carriages need to be secured, chemicals have to be neutralised or cleaned up and fires nearby any flammable material need to be controlled.

The accident happened in Germany, which means the German PPDR organization carry the responsibility to deal with the incident and coordinate the rescue efforts. Calls from the public to report the incident reach the relevant Belgian, Dutch and German command and control centres. As the relevant PPDR organizations in the region have bi-lateral incidence support agreements in place, the Belgian and Dutch PPDR organizations immediately offer resources to the relevant German authorities.

Administrative information is transmitted in a pre-agreed format to the relevant German command and control centre and includes capability information, such as what type of rescue equipment can be made available or what type of hazardous materials can be dealt with, as well as the MCX user IDs of the first responder able to operate the relevant equipment. The information transmitted includes an estimated time to reach the incident site.

Since the accident involves trains and rail equipment, the relevant rail authorities and support groups need to be contacted and brought into the rescue efforts.

In order to ensure operational safety of the first responders on-site and a quick response to on-site emergency calls, their respective MCX Service UE’s emergency call communication is reconfigured to be routed to a specific mobile on-site emergency call centre.

The relevant German command and control centre analyses the information received and requests the resources that are deemed necessary to support the rescue efforts. Information such as configuration data and authorizations are then transmitted back to the relevant Belgian and Dutch control centres and rail emergency command and control centre authorized user(s) to allow the relevant MCX UEs to affiliate with the relevant German MCX Service System talk groups.

This allows the multi-agency rescue and first response efforts to be coordinated efficiently and ensures communication is possible with all resources involved in the incident.

### 5.2.2 Pre-conditions

All relevant Belgian and Dutch MC UEs are equipped with roaming SIM cards, which allow the MC UEs to register in the German LTE/5GS networks. Capability information is linked to an MCX user ID record and by requesting a specific capability, such as “chemical incident”, “medical air lift” or “heavy equipment handling” the relevant resources can be made available by the partner organisations and MC UEs can be affiliated and linked to the relevant talk groups.

1. The Dutch and Belgian first responders have to have valid MCX subscriptions in their respective MCX Service Systems
2. MCX User capability information is available for efficient request/deployment of relevant resources
3. Connections between the relevant systems have been established that allow exchange of administrative configuration information

### 5.2.3 Service Flows

1. The relevant Dutch and Belgian command and control centres receive incident information from the public
2. The relevant Dutch and Belgian authorized user(s) analyse the response requirements, collect additional information which resources and capabilities are available
3. After it has been understood that the incident site is located in Germany, the authorized user(s) in the Dutch and Belgian MCX Service System establish contact via a separate administrative configuration protocol with the German MCX Service System
4. The train emergency system sends information about the incident to the relevant rail emergency command and control centre(s) or authorities
5. The relevant authorized user(s) in the Dutch and Belgian command and control centres inform the relevant German authorized user(s) which resources, such as heavy lifting machinery, air lift, fire engines or ambulances and capabilities, such as handling chemical spills or weight limitations for lifting equipment are available and when they could be available at the incident site
6. The relevant authorized user(s) in the German Primary MCX Service System collect the information and either automatically or manually, processes the information and request the required resources and capabilities from the Dutch and Belgian MCX Service Systems, plus the relevant rail authorized user(s)
7. The Dutch, Belgian MCX Service Systems and relevant rail authorized user(s) exchange the relevant administrative and security information via the separate administrative configuration protocol with the German MCX Service System
8. After acceptance or successful checks/authorisations, user profiles of the Dutch and Belgian and rail incident support MCX Service Users are updated to include the relevant information, such as user group configuration and encryption key material, assigned by the German MCX Service System
9. The Dutch, Belgian MCX Service Users UEs affiliate to the German MCX Service Groups via the Dutch and Belgian MCX Service System and their Group communication is routed from the public German LTE/5GS through the Dutch and Belgian MCX Service System to the German MCX Service System
10. The relevant rail incident support MCX Service Users UEs affiliate to the incident related and relevant MCX Service Groups

### 5.2.4 Post-conditions

1. First responders from the Dutch and Belgian MCX Service organizations can select and participate in the relevant German talk groups
2. The relevant rail authorities, key personnel and first responders can participate in the MCX services (MCPTT, MCVideo and MCData) with the relevant authorized MCX Services Users

### 5.2.5 Existing features partly or fully covering the use case functionality

The following requirements refer to 3GPP TS 22.280.

[R-5.6.2.2.1-013] The MCX Service shall provide a mechanism for an MCX Service Administrator to configure which MCX Service Group (i.e., user's selected group or dedicated MCX Service Emergency Group) is used for the MCX Service Emergency Group Communication by an MCX User.

The following requirements refer to 3GPP TS 33.180.

Clause 5.1.5 MC user migration service authentication and authorisation.

### 5.2.6 Potential New Requirements needed to support the use case

[PR 5.2.6.1] An MCX Service shall provide secure mechanisms to allow an authorised MCX User to request configuration information from Partner MCX Service Systems.

[PR 5.2.6.2] An MCX Service shall provide secure mechanisms to allow an authorised MCX User to send configuration information to Partner MCX Service Systems.

[PR 5.2.6.3] An MCX Service shall provide secure mechanisms to allow an authorised MCX User to exchange MCX User relevant information with Partner MCX Service Systems.

# 6 Security Aspects

## 6.1 Introduction

This section proposes potentially new security requirements that allow Primary and Partner MCX Service Systems to exchange administrative and security relevant information without compromising integrity of the connected MCX Service Systems.

## 6.2 Potential requirements

[PR 6.2.001] Exchange of administrative and security related information between MCX Service systems shall not compromise the integrity and security of either MCX Service System.

[PR 6.2.002] Exchange of administrative and security related information shall not expose the internal structure or configuration of either MCX Service System.

[PR 6.2.003] MCX Service Systems shall detect and prevent unauthorized connection attempts

[PR 6.2.004] Exchange of administrative and security related information between MCX Service Systems shall cover prevention of replay attacks

[PR 6.2.005] Exchange of administrative and security related information between MCX Service Systems shall cover algorithm negotiation and prevention of bidding down attacks

[PR 6.2.006] Mutual authentication and authorization between the connected MCX Service Systems shall be supported

[PR 6.2.007] Separate, mutual authentication and authorization shall be possible with more than one MCX Service System at any time

[PR 6.2.008] Messages that travers trust boundaries shall follow 3GPP specifications for protection, if not protected by end-to-end security

# 7 Additional considerations

 Editor’s note: Add clauses as needed. Text to be provided.

# 8 Consolidated Potential Requirements

## 8.1 Changing group membership in a Partner MCX Service System

Table 8.1-1 – Changing group membership in a Partner MCX Service System - Consolidated Requirements

| CPR # | Consolidated Potential Requirement | Original PR # | Comment |
| --- | --- | --- | --- |
| CPR 8.1 | An MCX Service shall provide a mechanism to allow an authorised MCX User to request MCX User configuration changes in one or more Partner MCX Service Systems. | PR 5.1.6.1 | CPR 8.1 identical to PR 5.1.6.1 |
| CPR 8.2 | An MCX Service shall provide a mechanism to allow an authorised MCX User to evaluate and respond to requests for configuration changes from Partner MCX Service Systems. | PR 5.1.6.2 | CPR 8.2 identical to PR 5.1.6.2 |
| CPR 8.3 | An MCX Service shall provide a mechanism to allow an authorised MCX User to configure automatic responses to categories of requests for configuration changes from Partner MCX Service Systems. | PR 5.1.6.3 | CPR 8.3 identical to PR 5.1.6.3 |

## 8.2 Incident response involving multiple countries

Table 8.2-1 – Incident response involving multiple countries - Consolidated Requirements

| CPR # | Consolidated Potential Requirement | Original PR # | Comment |
| --- | --- | --- | --- |
| CPR 8.4 | An MCX Service shall provide a mechanism to allow an authorised MCX User to request configuration information from Partner MCX Service Systems. | PR 5.2.6.1 | CPR 8.4 identical to PR 5.2.6.1 |
| CPR 8.5 | An MCX Service shall provide a mechanism to allow an authorised MCX User to send configuration information to Partner MCX Service Systems. | PR 5.2.6.2 | CPR 8.5 identical to PR 5.2.6.2 |
| CPR 8.6 | An MCX Service shall provide a mechanism to allow an authorised MCX User to exchange operational MCX User relevant information, e.g. MCX User capability information, with Partner MCX Service Systems. | PR 5.2.6.3 | Original PR: An MCX Service shall provide secure mechanisms to allow an authorised MCX User to exchange MCX User relevant information with Partner MCX Service Systems. |

## 8.3 Security Aspects

Table 8.3-1 – Security Aspects - Consolidated Requirements

| CPR # | Consolidated Potential Requirement | Original PR # | Comment |
| --- | --- | --- | --- |
| CPR 8.7 | Exchange of administrative and security related information between MCX Service systems shall not compromise the integrity and security of either MCX Service System. | PR 6.2.001 | CPR 8.7 identical to PR 6.2.001 |
| CPR 8.8 | Exchange of administrative and security related information shall not expose the internal structure or configuration of either MCX Service System. | PR 6.2.002 | CPR 8.8 identical to PR 6.2.002 |
| CPR 8.9 | Exchange of administrative and security related information between interconnected MCX Service systems shall be secure. | PR 6.2.003 | Original PR: MCX Service Systems shall detect and prevent unauthorized connection attempts |
| CPR 8.9 | Merged into [CPR 8.9] | PR 6.2.004 |  |
| CPR 8.9 | Merged into [CPR 8.9] | PR 6.2.005 |  |
| CPR 8.9 | Merged into [CPR 8.9] | PR 6.2.006 |  |
| CPR 8.9 | Merged into [CPR 8.9] | PR 6.2.007 |  |
| CPR 8.9 | Merged into [CPR 8.9] | PR 6.2.008 |  |

# 9 Conclusions and Recommendations

This study has examined a number of use cases that form the basis for the consolidated potential requirements identified in clause 8.

It is proposed to consider the content in clause 8 as a basis for normative work in Rel-18 to support requirements to enable the exchange of administrative configuration and security relevant information between interconnected MCX Service systems.

# Annex <A>:<Title>

Annex <B> (informative):
Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2019-11 | SA1#88 | S1-193222 |  |  |  | First revision | 0.2.0 |
| 2020-09 | SA1#91e | S1-203233 |  |  |  | Addition of Overview clause | 0.3.0 |
| 2020-09 | SA1#91e | S1-203310 |  |  |  | Addition of use case – change group membership in Partner MCX Service System | 0.3.0 |
| 2020-09 | SA1#91e | S1-203311 |  |  |  | Addition of Security Aspects and Potential requirements | 0.3.0 |
| 2021-03 | SA1#93e | S1-210164 |  |  |  | Addition of use case - Incident response involving multiple countries | 0.4.0 |
| 2021-03 | SA1#93e | S1-210166 |  |  |  | Clarification for clauses 5.1.1, 5.1.2, 5.1.3 | 0.4.0 |
| 2021-05 | SA1#94e | S1-211395 |  |  |  | Addition of content in clause 8, Consolidated potential requirements | 0.5.0 |
| 2021-05 | SA1#94e | S1-211084 |  |  |  | Addition of content in clause 9, Conclusions and recommendations | 0.5.0 |
| 2021-06 | SA#92e | SP-210506 |  |  |  | Raised by MCC to v.1.0.0 for one-step approval | 1.0.0 |
| 2021-06 | SA#92e | SP-210506 |  |  |  | Raised by MCC to v.18.0.0 following one-step approval | 18.0.0 |
| 2021-06 | SA#92e | SP-210506 |  |  |  | Corrected logo (5G->5GA) | 18.0.1 |
| 2021-12 | SP-94 | SP-211496 | 0001 |   | D | Table linking CPRs to their PRs and use cases | 18.1.0 |