3GPP TR 23.715 V16.0.0 (2018-09)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Study on system enhancements for provision of access to

restricted local operator services by an unauthenticated

User Equipment (UE)

(Release 16)

** 

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

Keywords

3GPP, access, authentication, enhancements, services

***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.

© 2018, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

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

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

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

Contents

Foreword 5

1 Scope 6

2 References 6

3 Definitions, symbols and abbreviations 6

3.1 Definitions 6

3.2 Symbols 7

3.3 Abbreviations 7

4 Architectural Assumptions and Requirements 7

4.1 Architectural Assumptions 7

4.2 Architectural Requirements 8

5 Key Issues for EPC 8

5.1 Key Issue #EPC-1: Network indicating support for Restricted Local Operator Services and related UE behaviour 8

5.2 Key Issue #EPC-2: RLOS request indication 8

5.3 Key Issue #EPC-3: Support of unauthenticated UEs access to RLOS 8

5.4 Key Issue #EPC-4: Support of authenticated UEs access to RLOS 9

5.5 Void 9

5.6 Key Issue #EPC-6: Collection of charging information 9

5.7 Key Issue #EPC-7: Level of security 9

6 Key Issues for IMS 9

6.1 Key issue #IMS-1: Support for unauthenticated and authenticated user 9

6.2 Key issue #IMS-2: Identification of Restricted Local Operator Services at IMS layer 9

6.3 Key issue #IMS-3: Handling IMS session for Restricted Local Operator Service 10

6.4 Key issue #IMS-4: Support of emergency services by UEs attached for RLOS 10

7 Solutions 10

7.1 Solution #1: New SIB indicating support for Restricted Local Operator Services 10

7.1.1 Functional Description 10

7.1.2 Procedures 10

7.1.3 Impact on existing entities and interfaces 10

7.2 Solution #2: EPC attach/PDN connection for RLOS from unauthenticated/authenticated UE 11

7.2.1 Functional Description 11

7.2.2 Procedures 11

7.2.2.2 Detach procedure 12

7.2.3 Impact on existing entities and interfaces 12

7.3 Solution #3: IMS procedures for RLOS 12

7.3.1 Functional Description 12

7.3.2 Procedures 12

7.3.3 Impact on existing entities and interfaces 13

7.4 Solution #4: EPC solution using dedicated RLOS-APN 13

7.4.1 Functional Description 13

7.4.2 Procedures 15

7.4.2.1 Attach procedure 15

7.4.2.2 UE-initiated Detach procedure 17

7.4.2.3 MME-initiated Detach procedure 17

7.4.2.4 S1-based handover procedure 18

7.4.2.5 UE requested PDN connectivity 18

7.4.3 Impact on existing entities and interfaces 18

7.5 Solution #5: IMS solution with dedicated RLOS-APN and RLOS-specific P/S-CSCF 18

7.5.1 Functional Description 18

7.5.2 Procedures 19

7.5.2.1 IMS registration 19

7.5.2.2 Location Information retrieval 20

7.5.2.3 UE initiated RLOS IMS session establishment 20

7.5.3 Impact on existing entities and interfaces 21

7.6 Solution #6: Solution to key issue #EPC-3 & #EPC-4 to enable IMS calls after initial attachment 21

7.6.1 Functional Description 21

7.6.2 Procedures 22

7.6.2.1 UEs in Limited Service State that cannot be authenticated 22

7.6.3 Impact on existing entities and interfaces 22

7.7 Solution #7 to key issues #IMS-1, #IMS-2, and #IMS-3: IMS support for RLOS users 23

7.7.1 Functional Description 23

7.7.2 Procedures 24

7.7.3 Impact on existing entities and interfaces 24

7.8 Solution #8: Solution to key issues #IMS-4: Support of emergency services by UEs attached for RLOS 25

7.8.1 Functional Description 25

7.8.2 Procedures 25

7.8.2.1 UE performs detach from RLOS and then do emergency Attach 25

7.8.2.2 UE stays RLOS attached, and establishes emergency PDN connection 26

7.8.3 Impact on existing entities and interfaces 27

7.9 Solution #9: PLMN selection, radio access for RLOS and overload handling 27

7.9.1 Functional Description 27

7.9.2 Procedures 28

7.9.3 Impact on existing entities and interfaces 28

7.10 Solution #10: IMS solution with dedicated RLOS-APN and skipping IMS registration 28

7.10.1 Functional Description 28

7.10.2 Procedures 30

7.10.2.1 IMS registration 30

7.10.2.2 Location Information retrieval 30

7.10.2.3 UE initiated RLOS IMS session establishment 30

7.10.3 Impact on existing entities and interfaces 31

7.11 Solution #11: Partial security solution for key issue #EPC-7 31

7.11.1 Functional Description 31

7.11.2 Procedures 31

7.11.3 Impact on existing entities and interfaces 31

8 Evaluation 32

9 Conclusions 36

Annex <A>: Change history 38

# 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.

# 1 Scope

The objective of this Technical Report is to identify and evaluate potential architecture enhancements of EPS and IMS needed to support Provision of Access to Restricted Local Operator Services by Unauthenticated UEs as identified in TS 22.101 [2], TS 22.115 [3] and TS 22.228 [4], and determine which of the solutions can proceed to normative specifications.

This feature is only applicable to EPS 3GPP access. Access to local operator services does not affect the UICC.

# 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 22.101: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Service aspects; Service principles".

[3] 3GPP TS 22.115: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service aspects; Charging and billing".

[4] 3GPP TS 22.228: "3rd Generation Partnership Project; Service requirements for the IP multimedia core network subsystem".

[5] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[6] 3GPP TS 23.203: "Policies and Charging control architecture; Stage 2".

[7] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[8] 3GPP TS 23.167: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; IP Multimedia Subsystem (IMS) emergency sessions".

[9] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[10] 3GPP TS 22.011: "Technical Specification Group Services and System Aspects; Service accessibility".

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 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 TR 21.905 [1].

**Restricted local operator services**: communication services provided by an operator that involve either automated or human assistance (e.g. credit card billing, directory assistance, customer care) for which successful authentication is not necessary.

## 3.2 Symbols

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

Symbol format (EW)

<symbol> <Explanation>

## 3.3 Abbreviations

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

RLOS Restricted Local Operator Services

# 4 Architectural Assumptions and Requirements

## 4.1 Architectural Assumptions

The goal of the study is to enable access to those Restricted Local Operator Services (RLOS), however the definition of such restricted local operator services offered by an operator is out of scope of 3GPP.

Architectural assumptions are the following:

- Access to RLOS is only possible for UEs when using EPC via E-UTRAN as IPCAN.

- Both unauthenticated UEs and authenticated UEs in limited service state can access RLOS via the same architecture.

An authenticated UE allowed to access EPC may access the same services that are provided as RLOS but in this case, it is not within the scope of RLOS. No work will be done in this area.

- The UE shall indicate to the EPC and the IMS network that the request is a request for RLOS.

- The standard shall support IMS emergency services for UEs attached for RLOS.

- Allowing access to RLOS is completely under the local operator's control.

- If the UE performs RLOS attach, the network may perform authentication if security information is available. Otherwise, authentication to EPC access for RLOS is skipped.

NOTE: whether authentication for EPC access for roaming UEs in limited state may be performed based on the presence of specific roaming agreements is to be stated in the conclusions in clause 9.

- The solution shall support both non-IMS and IMS RLOS services.

- When RLOS are accessed via IMS sessions:

1) they do not require any specific support for location over and above what is defined by IMS already;

2) they do not require any specific support regarding call back to the user that has initiated the session;

3) the IMS RLOS are securely isolated to avoid e.g. DOS attacks to IMS entities offering regular IMS services.

- Only UE-originated RLOS requests are supported.

- No support of multiple PDN connections for RLOS.

- No support of mobile terminated services.

- This feature is only applicable to EPS 3GPP access.

- Inter-RAT handovers and handover between 3GPP and non-3GPP accesses are not supported.

- The use of the RLOS feature does not impact the local service provider's ability to support LI.

## 4.2 Architectural Requirements

Editor's note: This clause will define the architectural requirements based on the normative stage-1 requirements defined in TS 22.101, TS 22.115 [3] and TS 22.228 [4] with regards to Provision of Access to Restricted Local Operator Services by Unauthenticated UEs.

# 5 Key Issues for EPC

## 5.1 Key Issue #EPC-1: Network indicating support for Restricted Local Operator Services and related UE behaviour

TS 22.101 [2] specifies: "When a UE recognizes an origination attempt to a restricted local operator service and has not received an indication from the serving system that restricted local operator services are available, the UE shall block the origination attempt."

This key issue addresses:

- how the PLMN announces its support of RLOS to all UEs;

- the behaviour of a supporting UE when it detects the network support of RLOS;

- the behaviour of a supporting UE when it does not detect the network support of RLOS.

NOTE: This key issue does not address the mechanisms for rejecting UE requests in case of an unauthorized attempt to access RLOS.

## 5.2 Key Issue #EPC-2: RLOS request indication

The solution shall address how unauthenticated and authenticated UEs indicate to the EPC that a request is for RLOS (e.g. at Attach);

## 5.3 Key Issue #EPC-3: Support of unauthenticated UEs access to RLOS

The solution shall address the EPC mechanisms required to support unauthenticated UEs. In particular, the following aspects are required to be studied:

- how to allow unauthenticated UEs to access EPC network for RLOS only if the EPC network supports RLOS;

- how to prevent unauthenticated UEs to access services which are not RLOS;

- how to minimize network congestion caused by unauthenticated UE access to RLOS in the RLOS enabled PLMN.

## 5.4 Key Issue #EPC-4: Support of authenticated UEs access to RLOS

The solution shall address the EPC mechanisms required to support authenticated UEs, in particular:

- how to allow authenticated UEs to access the same RLOS as unauthenticated UEs. This applies to UEs that the MME has successfully authenticated but the UE is not able to receive normal service (e.g. is in a forbidden area).

NOTE: Regularly attached UEs able to receive normal service may access the same services that are provided as RLOS but in this case, it is not within the scope of RLOS.

## 5.5 Void

## 5.6 Key Issue #EPC-6: Collection of charging information

The solution shall address how to collect charging information regarding the use of RLOS.

## 5.7 Key Issue #EPC-7: Level of security

The solution shall have a level of security, which should not be less than that which is currently applied to existing equivalent network access methods (e.g., unauthenticated emergency calling).

# 6 Key Issues for IMS

## 6.1 Key issue #IMS-1: Support for unauthenticated and authenticated user

The key issue here is that the network enables any UE access to a requested service through RLOS. This applies to all UEs, authenticated and non-authenticated.

The solution should use the same mechanisms for both unauthenticated and authenticated UEs as much as possible.

## 6.2 Key issue #IMS-2: Identification of Restricted Local Operator Services at IMS layer

The key issue here is that it is beneficial if IMS services allow clear service identification. For access to restricted local operator service this means that:

- the UE need to be able to determine the case and start session setup without requiring IMS registration for RLOS services. Further the UE will need to indicate to the IMS network that its request is for RLOS via appropriate information in the SIP request; and

- the core network functional entities need to be able to detect the specific information for an RLOS request.

The study will determine what to configure in the IMS network (e.g., phone number, captive portal), in which IMS entity(ies), and what to signal to the UE (e.g. specific CSCF address);

## 6.3 Key issue #IMS-3: Handling IMS session for Restricted Local Operator Service

At IMS layer, RLOS are always provided in the local PLMN without any involvement of the Home PLMN.

The key issue for the UE is to support initiating a session setup for RLOS without requiring IMS registration for RLOS services.

NOTE: UE only initiates IMS sessions for RLOS if the network has indicated support via signalling in the underlying layers.

The key issue for the IMS core network functional entities is to support session setup for RLOS from users without requiring IMS registration for RLOS services. Sessions for RLOS from authenticated and unauthenticated users are handled in the PLMN that provides the entry point into the IMS. This means that the IMS core network functional entities of the PLMN that provides the P-CSCF to which the UE is attached will handle the IMS session request locally.

## 6.4 Key issue #IMS-4: Support of emergency services by UEs attached for RLOS

The solution shall describe how a UE attached for RLOS can obtain emergency services.

# 7 Solutions

## 7.1 Solution #1: New SIB indicating support for Restricted Local Operator Services

### 7.1.1 Functional Description

This is a solution to key issue EPC-1 and EPC-3.

A new SIB provided by E-UTRAN indicates that the PLMN is configured to support Restricted Local Operator Services. An operator may decide to unset the SIB indicator e.g. using OAM to prevent access attempts from UEs for RLOS e.g. in case of network congestion. The PLMNs where RLOS is supported may be stored in UICC (or ME) for the UE.

### 7.1.2 Procedures

UE sees through SIB that PLMN supports Restricted Local Operator Services and only attempts to access RLOS if the SIB is signaled by the camped cell. The PLMNs where RLOS is configured to be supported may be configured from HPLMN stored in a new list in UICC (or ME) for the UE. The exact definition and format of such list and how it will be used for manual or automatic PLMN selection for RLOS, will be defined by CT WG1 and CT WG6.

Editor's note: Whether automatic PLMN selection needs to be supported for RLOS will be confirmed by CT WG1.

### 7.1.3 Impact on existing entities and interfaces

E-UTRAN and UE need to support a new SIB that indicates support for Restricted Local Operator Services. UE only attempts to access RLOS if the SIB is signaled by the camped cell at the time the UE is accessing the network. The setting and unsetting of RLOS shall not trigger paging for UEs operating in other (normal) services.

The PLMNs where RLOS is supported may be configured from HPLMN and stored in a new list in UICC (or ME) for the UE.

## 7.2 Solution #2: EPC attach/PDN connection for RLOS from unauthenticated/authenticated UE

### 7.2.1 Functional Description

This is a solution to key issue EPC-2, EPC-3, EPC-4 that defines Attach/Detach and PDN connectivity procedure for RLOS. The solution considers only the scenario where the UE requesting RLOS is unauthenticated, or the UE requesting RLOS is authenticated but in limited state.

### 7.2.2 Procedures



Figure 7.2.2-1: Attach/PDN connectivity procedure for RLOS

0. A new SIB provided by E-UTRAN indicates that PLMN supports Restricted Local Operator Services. See clause 7.1.

1. The UE sends an indication in Attach Request message that the Attach is for Restricted Local Operator Services (this is similar to the Emergency Attach indication that is used for "unauthenticated" UEs for emergency calls) which triggers the MME to select a locally configured APN that is used for RLOS.

In case of the authenticated UE (i.e. in limited state), the UE shall perform the detach procedure before step 1.

2. The UE does not need to be authenticated by the MME, IMSI (if available) and IMEI(SV) are retrieved from the UE.

3. MME sends a Create Session Request towards the PGW including the indication that is for RLOS (indication or APN) the IMSI (if available), and the IMEI(SV) as specified in TS 23.401 [5].

4. PGW establishes an IP-CAN session with the PCRF as described in TS 23.401 [5] and TS 23.203 [6]. The IP-CAN session is identified with UE's IPv4 address or IPv6 prefix associated with the PDN connection for RLOS. The IMSI (if available), and the IMEI(SV) are passed to the PCRF as part of the IP-CAN session establishment.

Duration of PDN connection for RLOS is controlled through local policies.

If needed the PGW returns back to the UE in a PCO the P-CSCF address used for RLOS using procedures defined in TS 23.228 [7] for P-CSCF discovery. The PGW shall block any traffic that is not from or to addresses of network entities (e.g. P-CSCF, captive portal) providing Restricted Local Operator Service.

5. UE completes the Attach or UE requested PDN connection procedure.

#### 7.2.2.2 Detach procedure

When the PGW initiates to delete the default bearer for RLOS, if emergency PDN connection is not established, the MME performs detach procedure as specified in TS 23.401 [5].

When the RLOS-attached UE has no emergency PDN connection, if UE is transferred to ECM-IDLE state, UE and Network shall implicitly detach without NAS signalling transactions. i.e. if the RRC connection is released after allowed inactivity period configured in E-UTRAN expires, the UE shall detach itself implicitly without sending detach request, and if S1-AP is released, the MME shall detach the UE without sending the detach request.

### 7.2.3 Impact on existing entities and interfaces

Impacts in UE and MME to implement the procedures defined in clause 7.2.2.

- UE: UE includes RLOS indication in Attach request for RLOS.

When RLOS-attached UE becomes ECM-IDLE, UE detaches implicitly without NAS transaction with MME.

- MME: MME selects the RLOS-dedicated APN to setup PDN connection, and may include RLOS indication to SGW/PGW.

When the UE attaches for RLOS, MME skips mutual Authentication procedure and location update to HSS.

When RLOS-attached UE becomes in ECM-IDLE state, MME detaches without NAS transaction with UE.

## 7.3 Solution #3: IMS procedures for RLOS

### 7.3.1 Functional Description

This is a solution to key issue IMS-1, IMS-2, IMS-3 that defines IMS procedure for RLOS.

### 7.3.2 Procedures



Figure 7.3.2-1: IMS procedure for RLOS

1. If the UE is unauthenticated in IMS it initiates IMS registration by sending a SIP REGISTER (UserID-1) message indicating that is IMS Registration for RLOS. The UserID-1 parameter is an IMPI and optionally an IMPU.

2. Upon reception of the SIP REGISTER message from the indication that the SIP REGISTER is for RLOS the P-CSCF determines that it is for RLOS. The P-CSCF may optionally request from the PCRF the EPS-level identities (e.g. IMSI, IMEI(SV)) in the Rx session establishment request. The PCRF performs session binding based on the UE's IP address/prefix (as defined in TS 23.203 [6] clause 6.1.1.2) and provides one or more EPS-level identities to the P-CSCF.

3. Based on operator configuration for RLOS, the GIBA procedure over Gm as defined in TS 24.229 [9] is performed, the P-CSCF responds with a 420 response with sec-agree value listed in the unsupported header field.

4. UE according to TS 24.229 [9], performs a new initial registration by sending a SIP REGISTER (UserID-2, IMEI) message and without inclusion of the Authorization header field. UserID-2 is an a public user identity derived from IMSI. P-CSCF may verify the IMSI/IMEI provided by the PCRF in step 7 against the IMSI/IMEI derived from the public user identity provided by the UE, prior to accepting the SIP REGISTER message.

5. P-CSCF accepts the registration with 200 OK. From the UE point of view, the procedure is the same as specified for GIBA (GPRS-IMS bundled authentication) procedures in TS 24.229 [9].

6. UE then attempts an RLOS session by sending a SIP INVITE (UserID-3) message. UserID-3 is set to UE's public identity.

7. The P-CSCF verifies whether the UserID-3 indicated in the SIP INVITE message. If compliant, P-CSCF forwards the SIP INVITE towards the Call Centre that is providing the RLOS.

Editor's note: It is FFS whether the P/S-CSCF or AS will restrict access only to the Restricted Local Operator Services.

### 7.3.3 Impact on existing entities and interfaces

Impacts in UE, P-CSCF and PCRF to implement the procedures in clause 7.3.2.

## 7.4 Solution #4: EPC solution using dedicated RLOS-APN

### 7.4.1 Functional Description

During the attach procedure:

- If the UE is not attached to the network and detects that the user is requesting RLOS, then the UE shall check whether the PLMN is advertising its support of RLOS to all UEs. If the PLMN does not advertise its support of RLOS, the UE shall block the origination attempt (according to TS 22.101 [2] clause 34.2). If the PLMN advertises its support of RLOS, the UE shall indicate in the Attach Request that the attachment is for RLOS.

If the UE is not in limited service state, it shall not initiate an Attach procedure with RLOS indication.

If the UE in limited service state initiates an Attach procedure with RLOS indication, and:

- If the MME already has valid credentials for the UE, the MME uses the existing credentials and consider the UE as authenticated for RLOS.

- If the MME does not have valid credentials for the UE and if the UE IMSI (retrieved by the MME) corresponds to the PLMN of the MME, then the MME shall proceed the attach procedure to retrieve the security information from the HSS which shall attempt to authenticate the UE. Whatever the authentication result, the MME shall proceed with the RLOS attach procedure: it establishes a default PDN connection to a specific RLOS APN as part of the Attach procedure, and accept the RLOS Attach request.

NOTE: Whether authentication for EPC access for roaming UEs in limited state may be performed based on the presence of specific roaming agreements is to be stated in the conclusions in clause 9.

- Otherwise, the MME shall skip the authentication, establish a default PDN connection to a specific RLOS APN as part of the Attach procedure, and accept the RLOS Attach request.

Session Management:

- The solution assumes that a specific RLOS-APN, unique for the PLMN and configured in the MME, is used.

- During attach, based on the presence of the RLOS indication in the NAS Attach Request, the MME may either select a specific RLOS PGW in the same PLMN, preconfigured in the MME RLOS Configuration Data or a dynamically allocated PGW in the same PLMN, based on a specific RLOS-APN.

- During PDN connection establishment, MME send RLOS APN to the SGW and the PGW. The PCRF derives that the PDN connection is for RLOS via the RLOS-APN.

- For IMS RLOS sessions, the PCRF may establish dedicated bearers.

- Because at the end of RLOS session, the UE should be detached, any of the following procedures triggers a UE Detach procedure:

- PDN GW initiated bearer deactivation, as described in clause 5.4.4.1 of TS 23.401 [5];

- UE initiated Detach procedure as described in clause 7.4.2.2 of TS 23.401 [5].

Idle mode mobility and handovers:

- During idle mobility involving MME change, as in emergency service, if the UE's IMSI is unauthenticated, the unauthenticated IMSI indication will be sent from the old/source MME to the new/target MME, and if the UE does not have a USIM, IMSI will not be included in Context Response as specified in TS 23.401 [5] clause 5.3.1.

- During handover involving MME change, as in emergency service, if the UE is RLOS attached and the UE does not have a USIM, IMSI cannot be included in the MME UE context in Forward Relocation Request message, and if the IMSI has not been authenticated previously, then the IMSI shall be marked as unauthenticated as specified in TS 23.401 [5] clause 5.5.1.2.

- No additional impact is expected.

Charging:

- Charging of RLOS PDN connections can be performed by OFCS and OCS as for regular PDN connections. The rating group provided by PCRF should just be a RLOS specific rating group. No changes are needed as the APN is known by the PCRF.

Location procedures:

- Location services are not invoked.

### 7.4.2 Procedures

#### 7.4.2.1 Attach procedure



Figure 7.4.2.1-1: Attach procedure

Attach procedure from Figure 5.3.2.1-1 applies, except for the following aspects:

1. If the UE has detected that the user is requesting RLOS, the UE shall check whether the PLMN is advertising its support of RLOS to all UEs. If the PLMN does not advertise its support of RLOS, the UE shall block the origination attempt (according to TS 22.101 [2] clause 34.2). If the PLMN announces its support of RLOS, the UE proceeds to attach by sending an Attach Request in which it indicates that the attachment is for RLOS (via e.g. Attach Type and/or Request Type) and it provides its IMSI (or its IMEI if the UE has no IMSI). The UE shall not identify itself with a temporary identity.

5a. If the MME is configured to support RLOS for unauthenticated IMSIs and the UE has indicated that the attach request is for RLOS (via e.g. Attach Type "RLOS"), the MME shall behave as described in clause 7.4.1.

5b. This step may be performed based on operator's policy.

8. For an RLOS Attach, the MME shall not send an Update Location Request to the HSS. However, when required as described in clause 7.4.1, the MME may retrieve security information from the HSS.

11. For an RLOS Attach, the MME shall not check for access restrictions, regional restrictions or subscription restrictions (e.g. CSG restrictions) and shall continue with the Attach procedure.

12. For an RLOS Attach, the MME applies the parameters from MME RLOS Configuration Data for the RLOS bearer establishment performed in this step and any potentially stored IMSI related subscription data are ignored by the MME. For initial RLOS Attach, the MME selects either a specific RLOS PGW in the same PLMN, preconfigured in the MME RLOS Configuration Data, or a dynamically allocated PGW in the same PLMN, based on a specific RLOS-APN. For RLOS attached UEs, IMSI is included if available and, if the IMSI has not been authenticated, then the IMSI shall be marked as unauthenticated. The RLOS characteristics of the default PDN connection (i.e. APN-AMBR, MBR, ARP) are pre-configured in the MME.

13. For RLOS attached UEs, IMSI is included if available and if the IMSI has not been authenticated then the IMSI shall be marked as unauthenticated.

14. The PDN GW and the PCRF determines that RLOS are requested based on the RLOS APN received in Create Session Request message. For RLOS attached UEs which are unauthenticated, the PDN GW provides the IMEI as the UE Identity instead of IMSI, to the PCRF. If the PCC is configured to support RLOS and if dynamic PCC is deployed, the PCRF, based on the RLOS APN, sets the ARP of the PCC rules to a value that is reserved for RLOS and the authorization of dynamic PCC rules.If dynamic PCC is not deployed, the PDN GW uses the ARP of the default RLOS EPS bearer for any potentially initiated dedicated RLOS EPS bearer.

17. The new MME sends an Attach Accept with RLOS indication. For an RLOS attached UE, i.e. for UEs that have only RLOS EPS bearers established, there is no AS security context information included in the S1 control messages and there is no NAS level security when the UE has not been authenticated.

18. Manual CSG selection is not supported when an RLOS has been initiated.

25. For a UE in limited service state, if the UE has indicated that the request of for RLOS (via e.g. Request Type set to "RLOS"), the MME shall not send any Notify Request to an HSS.

#### 7.4.2.2 UE-initiated Detach procedure

UE-initiated Detach procedure from Figure 5.3.8.2-1 of TS 23.401 [5] applies, except for the following aspects:

Step 1: Security procedures that may be invoked if the NAS message is used to establish the S1 connection are not performed in the case of RLOS attached UEs that were not successfully authenticated.

#### 7.4.2.3 MME-initiated Detach procedure

MME-initiated Detach procedure from Figure 5.3.8.3-1 of TS 23.401 [5] applies, except for the following aspects:

Step 1: For RLOS attached UEs, MME initiates implicit detach procedures when implicit detach timer specific to RLOS expires or the eNB notifies that the UE RRC connection is released. And the UE may detach implicitly from the network when the RRC connection is released.

#### 7.4.2.4 S1-based handover procedure

S1-based handover procedure from Figure 5.5.1.2.2-1 of TS 23.401 [5] applies, except for the following aspects:

Step 3: For RLOS attached UEs, if the IMSI has not been authenticated, then the IMSI shall be marked as unauthenticated. Also, in this case, security parameters are included only if available.

#### 7.4.2.5 UE requested PDN connectivity

An RLOS attached UE shall not initiate any PDN Connectivity Request procedure.

If the MME receives a PDN Connectivity Request from an RLOS attached UE, the MME shall reject this request.

### 7.4.3 Impact on existing entities and interfaces

UE:

- The UE shall check whether the PLMN is advertising its support of RLOS before requesting RLOS attach.

- When requesting RLOS, the UE shall verify that it is in limited service state. If the verification is successful, the UE shall include an RLOS indication in the Attach Request.

MME:

- The MME shall be configured with RLOS APN and associated RLOS implicit detach timer (and potentially with pre-configured PGW(s)).

- The MME shall behave as described in clause 7.4.1.

PDN GW and PCRF:

- No impact. Only existing configuration.

## 7.5 Solution #5: IMS solution with dedicated RLOS-APN and RLOS-specific P/S-CSCF

### 7.5.1 Functional Description

This solution is intended to solve key issues #IMS-1, #IMS-2, #IMS-3 and #IMS-4.

During the EPC attach procedure, based on the RLOS indication provided by the UE, the EPC establishes a PDN connection to a specific APN dedicated to RLOS (see solutions #2 and #4). As RLOS are always provided in the PLMN the UE is accessing, the UE needs to select a P-CSCF suitable for RLOS sessions in that PLMN. For that, the address of the suitable P-CSCF is provided in the PCO by the PGW during Attach procedure. This dedicated address enables the use of either a general-purpose P-CSCF or a RLOS-specific P-CSCF. Whether a general-purpose P-CSCF or a RLOS-specific P-CSCF is used depends on the operator wishes about IMS isolation.

In this solution, the P-CSCF may be configured with a range of IP addresses reserved for RLOS.

The UE, whatever it is unauthenticated or authenticated in limited service state, performs an IMS registration for RLOS by adding an RLOS indication in the SIP Register message (required for general-purpose P-CSCF to determine the IMS Register is for RLOS). If the UE has indicated RLOS, if the P-CSCF has been configured with a range of IP addresses reserved for RLOS, the P-CSCF verifies that the UE IP address is within that range. P-CSCF may also verify that the PDN connection has been established for the RLOS APN by querying the PCRF. If one of the above verification fails, the IMS registration is rejected. P-CSCF skips authentication as described in TS 23.167 [8] clause K.3 for IMS emergency sessions for roaming users in deployments without IMS-level roaming interfaces.

UE's IP address spoofing is still possible, but IP address spoofing is always possible for unauthenticated UEs in any solution, but proposed verifications minimize the risks as described below:

- the IP address would need to correspond to a PDN connection that corresponds to the RLOS APN.

When the UE is successfully IMS registered for RLOS, it can request RLOS IMS services. On receiving the SIP Invite for an UE that is IMS registered UE for RLOS, the P-CSCF shall route the SIP INVITE request to a specific RLOS-CSCF to satisfy the IMS network isolation requirement (similar principle as for emergency IMS calls, which uses a specific E-CSCF). Emergency calls are detected the same way as in a regular P-CSCF and, in this case, the SIP INVITE request is routed to the E-CSCF. If the P-CSCF has determined that it is not for an emergency service and if the RLOS-CSCF has determined that the UE SIP INVITE request if not for RLOS, the UE SIP INVITE request is rejected.

The UE may request RLOS IMS services as long as it is IMS registered for RLOS. If the IMS registration timer expires, UE can re-register as long as it is EPC attached to the RLOS APN. However, when the UE is detached from the EPC, the PCRF shall indicate it to the P-CSCF, which then deregisters the UE from IMS i.e. it removes the P-CSCF UE context.

When provided, the network provided location information conveyed from the EPC to the P-CSCF via PCRF shall be forwarded to the RLOS-CSCF.

Charging of RLOS IMS sessions is performed by the IMS network as for a regular IMS sessions.

**P-CSCF additional features for RLOS**

- The P-CSCF can be a RLOS-specific P-CSCF or a general-purpose P-CSCF.

- The P-CSCF detects whether the IMS registration request from an UE is for RLOS from the RLOS indication provided by the UE. The P-CSCF, if configured with a range of IP addresses reserved for RLOS, verifies that the UE IP address is within that range. P-CSCF may also verify that the PDN connection is established for RLOS attached by querying the PCRF. P-CSCF skips authentication as described in TS 23.167 [8] clause K.3 for IMS emergency sessions for roaming users in deployments without IMS-level roaming interfaces.

- The P-CSCF selects an E-CSCF if it detects that the UE has initiated an emergency session request, according to TS 23.167 [8] clause 7.3 (Emergency Session Establishment in the Serving IMS network). The P-CSCF shall also be able to detect non-UE detectable emergency sessions as specified in TS 23.167 [8] clause 7.2.

Editor's note: Details for non UE-detectable emergency calls are FFS.

- If available, the P-CSCF shall provide RLOS-CSCF with the NPLI received from the PGW via PCRF.

- When the P-CSCF receives an indication from the PCRF that the UE has been RLOS detached from EPC, it shall deregister the UE from IMS, i.e. it removes the P-CSCF UE context.

**PCRF additional features for RLOS**

- The PCRF shall reply to the request from P-CSCF asking whether the PDN connection was established for RLOS (i.e. to RLOS APN).

- When the UE is RLOS detached from the EPC, the PCRF shall indicate it to the P-CSCF.

**RLOS‑CSCF additional features for RLOS**

- Verifies that the RLOS indication from P‑CSCF is present.

- Routes RLOS session establishment requests to an appropriate destination including anonymous session establishment requests.

- Generates CDRs for RLOS.

### 7.5.2 Procedures

#### 7.5.2.1 IMS registration

The UE performs IMS registration for RLOS by adding a RLOS indication in the SIP Register message, which allows the P-CSCF to detect that the IMS registration is for RLOS. The P-CSCF, if the UE has indicated RLOS, shall verify that the UE is RLOS attached by querying the PCRF on whether the PDN connection used for IMS signalling was established for RLOS (i.e. to RLOS APN). P-CSCF skips authentication, except for local subscribers.

#### 7.5.2.2 Location Information retrieval

Not applicable.

#### 7.5.2.3 UE initiated RLOS IMS session establishment

The following flow contains a high-level description of the RLOS procedures.



Figure 7.5.2.3-1: UE initiated RLOS IMS session establishment

The following steps are performed:

1. The UE sends an Attach Request to the EPC including an RLOS indication. The EPC establishes a local break-out default PDN connection for RLOS to the RLOS specific APN and replies to the UE with an indication that the UE is attached for RLOS as well as with the address of a P-CSCF suitable for RLOS sessions (via PCO). The EPC also informs PCRF that the PDN connection is for RLOS. See solution #4 in the TR for details.

2. According to clause 7.5.2.1, the UE initiates an IMS registration request for RLOS to the P-CSCF whose address was received in the PCO during RLOS Attach. SIP Register message shall contain an RLOS indication. The P-CSCF , if configured through policies, if the UE has included RLOS indication in the SIP Register message, it shall verify that, if P-CSCSF is configured with a range of IP addresses reserved for RLOS, the UE IP address is within that range. It may also verify that the PDN connection is for RLOS APN. If one of the above verifications fails, the IMS registration is rejected. P-CSCF verifies whether the UE is a subscriber of the local operator (via e.g. looking at the IMS domain).

If the user is an IMS subscriber of the local operator, P-CSCF send the IMS registration to the RLOS-CSCF (i.e. the local S-CSCF) to retrieve the IMS subscriber security information, otherwise, P-CSCF skips the authentication as described in TS 23.167 [8] clause K.3 for IMS emergency sessions for roaming users in deployments without IMS-level roaming interfaces.

3. If the UE requests RLOS, it sends a SIP INVITE for the establishment of an IMS RLOS session with an RLOS indication. The P-CSCF routes the SIP request to the RLOS specific CSCF. Emergency calls are detected the same way as in a regular P-CSCF, and in this case the SIP request is routed to the E-CSCF.

### 7.5.3 Impact on existing entities and interfaces

## 7.6 Solution #6: Solution to key issue #EPC-3 & #EPC-4 to enable IMS calls after initial attachment

### 7.6.1 Functional Description

There are two options to support RLOS services through the RLOS APN.

In the first option, the RLOS APN can lead to a portal that guides the user to various services, and after that, the user can establish the VoLTE session. It is assumed that the SIP signalling in this case may not acquire the QCI 5 that would typically be associated with an APN dedicated for IMS. It is up to the discretion of the operator to associate the necessary QCI for the RLOS APN in this option. The operation of the portal, its functionalities, and its interactions with the UE are out of scope.

In the second option, the RLOS APN may lead directly to the IMS network to initiate the requested IMS service. The IMS network can be a regular IMS network provided that there is sufficient protection to ensure that RLOS users cannot acquire any service other than RLOS or can be a network dedicated to provide only RLOS.

It is up to operator policies to select the option it desires.

This is supported thanks to the following behaviour:

1. If the operator only allows non-IMS RLOS, the PGW does not provide the UE with P-CSCF address in the PCO. In this case, the UE is redirected to a portal when sending data.

2. If the operator allows both IMS and non-IMS RLOS, the PGW provides the UE with P-CSCF address in the PCO. In such case, the UE attempts to IMS register with RLOS indicationThe IMS register with RLOS indication is accepted by the IMS network. The UE may send an IMS session request.

3. When the IMS network receives the IMS session request, it may either redirect the UE to a portal (in which case, after exchanges with the portal, the UE may attempt to attempt IMS sessions again), or it may proceed with the IMS session request.

All exchanges with the portal are out of scope.

### 7.6.2 Procedures

#### 7.6.2.1 UEs in Limited Service State that cannot be authenticated



Figure 7.6.2-1: IMS access following Attach/PDN connectivity procedure for Unauthenticated UEs

1. UE attaches to EPC with RLOS indication.

2. MME skips authentication.

3. MME initiates Create Session Request to the SGW/PGW for the RLOS APN.

4. EPC attachment to the RLOS APN is completed.

5. Option 1: If the UE received a P-CSCF address in the PCO, the UE performs IMS Registration. Otherwise, the UE is redirected to a portal when sending data.

6. The UE attempts to initiate the RLOS IMS session and the IMS network may either proceed with the IMS session request or redirect the IMS request to e.g. an announcement machine, which instructs the UE to initiate a web page.

7. The UE is connected to the portal and performs (transparently to EPS) any exchanges with the portal.

8. Option 2: UE attempts to initiate the RLOS IMS session and is successful.

NOTE: It is out of scope how IMS determines to route an RLOS IMS session to an announcement or completes the session.

### 7.6.3 Impact on existing entities and interfaces

This solution requires a new RLOS indication be carried in an initial attach. The following nodes are impacted:

MME:

- MME supports RLOS indication from the UE;

- MME supports configuration of RLOS APN and use this APN for RLOS attach.

## 7.7 Solution #7 to key issues #IMS-1, #IMS-2, and #IMS-3: IMS support for RLOS users

### 7.7.1 Functional Description

Three RLOS scenarios are addressed in this solution from an IMS network point of view:

- In the first scenario, RLOS UEs are allowed to make VoLTE calls even if their IMS registration cannot be performed (UEs belonging to an external domain). In this case a temporary registration record will be created for the UE in the S-CSCF and P-CSCF with a default profile and tagged as "unauthenticated external subscriber". The temporary record is kept for a period determined by local policies.

- In the second scenario, RLOS UEs are allowed to make VoLTE calls even if their IMS registration failed. This is the case for the operator own IMS subscribers who failed authentication. In this case a temporary registration record will be created for the UE in the S-CSCF and P-CSCF with a default profile and tagged as unauthenticated own subscriber. The temporary record is kept for a period determined by local policies.

- In the third scenario, RLOS UEs are successfully authenticated (Operator own IMS subscribers) and are registered in IMS. These RLOS UEs are depicted as authenticated IMS RLOS UEs.

All IMS nodes performing registration are in the local operator.

Editor's note: The usage of P-Asserted-Identity will be included in the normative phase.

Editor's note: Whether P-CSCF or S-CSCF initiates 420 for GIBA is to be confirmed.

To address the above scenarios, a UE desiring access to RLOS must perform regular IMS registration with the P-CSCF and must include a feature tag to indicate its request for RLOS.

**For scenario 1 (subscribers belonging to external domain) :** If the P-CSCF realizes that the UE is not its own subscriber based on the registering IMS identity, it selects a S-CSCF supporting RLOS configured in it and forwards the SIP Registration to the S- CSCF. The S-CSCF knowing that the registering UE is not its own subscriber sends back to the UE a 420 if the S-CSCF supports GIBA or 403 (forbidden) if it does not support GIBA.

If the UE receives 403, it can still initiate an RLOS IMS session, and shall include an RLOS indication in the IMS session.

If the UE receives 420 and supports GIBA, it sends back a new SIP Register request to which the S-CSCF responds with a 200 OK. The UE can subsequently initiate an RLOS IMS session and shall include an "RLOS indication" in the IMS session. The UE can refresh the registration based on the received timer from S-CSCF following normal IMS re-registration procedures.

If the UE receives 420 and does not support GIBA, the UE can subsequently initiate an RLOS IMS session, and shall include an "RLOS indication" in the IMS session.

No I-CSCF is involved for case 1.

**For scenario 2 (UE own subscribers that cannot be successfully authenticated):** If the P-CSCF realizes that the UE is its own subscriber based on the registering IMS identity, it performs normal IMS registration procedure, forwards the IMS registration to an I-CSCF which selects a S-CSCF that supports RLOS and forewords the registration to the selected S-CSCF. The S-CSCF challenges the UE with a 401 response. The UE sends a new SIP Register request and if the authentication fails, then the S-CSCF returns a 403 forbidden response to the UE.

If the UE receives 403, it can still initiate an RLOS IMS session, and shall include an RLOS indication in the IMS session.

**For scenario 3 (UE own subscribers that are successfully authenticated):** If the P-CSCF realizes that the UE is its own subscriber based on the registering IMS identity, it performs normal IMS registration procedure, forwards the IMS registration to an I-CSCF which selects a S-CSCF that supports RLOS and forewords the registration to the selected S-CSCF. The S-CSCF challenges the UE with a 401 response. The UE sends a new SIP Register request and if the authentication is successful, then the S-CSCF returns a 200 OK to the UE, and a security association shall be established between the UE and P-CSCF.

The UE can than initiate RLOS IMS sessions and shall include an RLOS indication in the IMS session. The S-CSCF in this case bypasses originating services.

NOTE: P-CSCF may be, based on operator policy, be configured with different policies for all of the above 3 cases which limits the set of destinations for authenticated and unauthenticated IMS RLOS UEs that it needs to enforce. The P-CSCF relies on the feature tag, depicting RLOS support, included in the IMS registration to enforce these policies. The applicable lists for both authenticated and unauthenticated UEs may be different.

A P-CSCF supporting RLOS can also be used for regular IMS UEs.

The support for emergency calls is described in other solutions

### 7.7.2 Procedures

This will be handled during the normative phase.

### 7.7.3 Impact on existing entities and interfaces

The solution impacts the following nodes:

**UE:**

An UE desiring access to RLOS must include a feature tag at IMS registration to indicate its support to RLOS. An UE that receives a 403 forbidden as a response to an IMS registration can still initiate an RLOS IMS session.

An UE that receives a 420 response to an IMS registration and does not support GIBA, can still initiate an RLOS IMS session.

In all cases, the UE shall include an RLOS tag in the RLOS IMS session initiation request.

**P-CSCF:**

The P-CSCF must understand the new RLOS feature tag.

The P-CSCF may be configured with the list of RLOS services to enforce originating sessions for all three cases discussed above.

The P-CSCF must support incoming RLOS sessions for all three cases discussed above.

The P-CSCF must create the temporary registration records with default profile for UEs belonging to an external domain or its own subscribers that failed authentication.

The P-CSCF must be configured with a list of S-CSCF(s) that support RLOS for forwarding an incoming registration from a UE belonging to an external domain.

The P-CSCF must insert the RLOS tag for a RLOS IMS session if the UE does not include one.

**S-CSCF:**

The S-CSCF shall route an incoming RLOS to its target for UEs belonging to the 3 cases described above. For successfully authenticated UEs for the operator own subscribers, no originating services shall be permitted.

The S-CSCF shall include in the CDR an RLOS tag for all three cases described above.

**I-CSCF:**

I-CSCF must understand the new capabilities related to RLOS and allocate a S-CSCF supporting RLOS at IMS registration when the IMS Register request includes the RLOS feature tag.

**HSS:**

HSS must support enabling a S-CSCF to declare RLOS as supporting capability

The Gm interface shall be enhanced to enable conveying the RLOS indicator.

Cx interface shall support new RLOS capability.

## 7.8 Solution #8: Solution to key issues #IMS-4: Support of emergency services by UEs attached for RLOS

### 7.8.1 Functional Description

For a UE that is already attached for RLOS services, if the user would like to request an emergency service, the UE may detach from RLOS and then do emergency Attach, or the UE may decide to stay RLOS attached and to establish an emergency PDN connectivity towards the emergency APN, depending on the UE state (e.g. UE with or without USIM, authenticated or not authenticated).

Editor's note: Whether one of the solutions is sufficient or both solutions should be supported is FFS. Details on what the UE behaviour is for a given UE state are FFS.

After the emergency attach is completed or after the emergency PDN connection is established, the UE shall perform IMS emergency registration.

### 7.8.2 Procedures

#### 7.8.2.1 UE performs detach from RLOS and then do emergency Attach

In this procedure:

- For a UE without USIM, after the UE has been detached from the RLOS, the emergency EPS attach will be allowed only if behaviour d) of emergency bearer service support as specified in clause 4.13.12 in TS 23.401 [5] is supported.

- For a UE with USIM but unauthenticated, after the UE has been detached from the RLOS, the emergency EPS attach will be allowed if behaviours c) or d) of emergency bearer service support as specified in clause 4.13.12 in TS 23.401 [5] are supported.

- For a UE, which is authenticated but in limited service state, after detached from the RLOS, the emergency EPS attach will be allowed if behaviour b), c) or d) of emergency bearer service support as specified in clause 4.13.12 in TS 23.401 [5] are supported.



Figure 7.8.2.1-1 UE detach from RLOS and perform emergency Attach

1. An UE is RLOS attached.

2. The user would like to make an emergency call.

3. UE performs Detach from RLOS.

4. UE then perform emergency Attach as specified in TS 23.401 [5].

5. UE performs IMS emergency registration as specified in TS 23.167 [8].

### 7.8.2.2 UE stays RLOS attached, and establishes emergency PDN connection

In this procedure:

- For a UE without USIM, when attached with RLOS, the establishment of an emergency PDN connection will be allowed only if behaviour d) of emergency bearer service support as specified in clause 4.13.12 in TS 23.401 [5] is supported.

- For a UE with USIM but unauthenticated, when attached with RLOS, the establishment of an emergency PDN connection will be allowed if behaviours c) or d) of emergency bearer service support as specified in clause 4.13.12 in TS 23.401 [5] are supported.

- For a UE, which is authenticated but in limited service state, when attached with RLOS, if behaviour c) or d) of emergency bearer service support as specified in clause 4.13.12 in TS 23.401 [5] are supported, the establishment of an emergency PDN connection will be allowed.

- If behaviour b) in clause 4.13.12 of TS 23.401 [5] is supported, as authentication is skipped during RLOS attach, the establishment of an emergency PDN connection will be rejected by the network



Figure 7.8.2.2-1: RLOS attached UE initiate emergency service by establishing emergency PDN connection

1. An UE is RLOS attached.

2. The user would like to make an emergency call.

3. UE initiates UE requested PDN Connectivity with request type = Emergency, as specified in TS 23.401 [5].

4. After the emergency PDN connection is established, the UE performs IMS emergency registration, as specified in TS 23.167 [8].

### 7.8.3 Impact on existing entities and interfaces

The solution impacts the following nodes:

**UE**:

A UE is RLOS attach shall be able to detach from RLOS and then do emergency attach, or initiate emergency PDN connection when UE stays RLOS attached, and then perform emergency IMS registration.

**MME**:

Support of emergency PDN connection for an RLOS attached UE.

## 7.9 Solution #9: PLMN selection, radio access for RLOS and overload handling

### 7.9.1 Functional Description

This solution partially addresses Key Issues EPC-1 and EPC-2.

The solution is described as follows:

- The E-UTRAN is configured to broadcast system information about the support of RLOS in the PLMN, e.g. as described in Solution #1 in clause 7.1.

- If the user requests RLOS access and there are more than one PLMNs supporting RLOS, then the UE selects one of the available PLMNs either a) based on the user input solicited through the User Interface, or b) other ME configuration. Once a PLMN has been selected, this PLMN of the current serving cell is considered as the selected PLMN.

- During the RRC connection establishment procedure, the UE indicates in the RRC signalling that the RRC connection is for RLOS access, using RLOS RRC establishment cause. Based on the RLOS indication in the RRC signalling, the RAN node applies the following:

- The E-UTRAN may admit the radio access resources and the E-UTRAN may apply access control (e.g. in case of RAN overload or congestion control) for UEs accessing RLOS services. The E-UTRAN may reject the RRC connection establishment with extended wait timer. UE shall not attempt to establish a new RRC connection with RLOS RRC establishment cause, in the same PLMN but the UE can establish RRC connection for other services e.g. emergency or normal service. How E-UTRAN determines to reject RLOS request is implementation specific; and

- The E-UTRAN may select an appropriate MME serving the RLOS access to EPC. The RAN node forwards the NAS message from the UE to the selected MME.

NOTE 1: The use of RLOS specific MME is one way to limit the impact to "normal" UEs when massive signalling for RLOS is originated from unauthenticated UEs or authenticated UEs in limited service state.

NOTE 2: The RAN WGs will specify whether a new RRC Establishment Cause or another indication is used in the RRC signalling.

### 7.9.2 Procedures

Editor's note: This clause will describe the high-level procedures and information flows for the solution.

### 7.9.3 Impact on existing entities and interfaces

Impacts to UE:

- UE is able to process new SIB indication;

- UE is able to indicate request for RLOS service at RRC and at NAS layer;

- UE NAS layer may interact with the GUI for PLMN selection.

Impacts to RAN:

- E-UTRAN broadcasts RLOS SIB indication;

- E-UTRAN may apply RLOS-specific access control and reject RRC signalling requests with extended wait time;

- E-UTRAN node (e.g. eNB) is able to select CN node (e.g. MME) based on RLOS indication.

## 7.10 Solution #10: IMS solution with dedicated RLOS-APN and skipping IMS registration

### 7.10.1 Functional Description

This solution is intended to solve key issues #IMS-1, #IMS-2, #IMS-3 and #IMS-4. It reuses most of the principles used in emergency sessions for unauthenticated and authenticated UEs specified in TS 23.167 [8].

During the EPC attach procedure, based on the RLOS indication provided by the UE, the EPC establishes a PDN connection to a specific APN dedicated to RLOS (see solutions #2 and #4). As RLOS are always provided in the PLMN the UE is accessing, the UE needs to select a P-CSCF suitable for RLOS sessions in that PLMN. For that, the address of the suitable P-CSCF is provided in the PCO by the PGW during Attach procedure. This dedicated address enables the use of either a general-purpose P-CSCF or a RLOS-specific P-CSCF. Whether a general-purpose P-CSCF or a RLOS-specific P-CSCF is used depends on the operator wishes about IMS isolation.

In this solution, the P-CSCF may be configured with a range of IP addresses reserved for RLOS.

The UE, whatever it is unauthenticated or authenticated in limited state, skips the IMS registration procedure for RLOS. This is similar to emergency calls for UEs in limited state or when authentication fails specified in TS 24.229 [9] clause 4.7.2.

On receiving the SIP INVITE for an IMS emergency session with a RLOS indication, the P-CSCF, if configured with a range of IP addresses reserved for RLOS, verifies that the UE IP address is within the range of IP addresses reserved for RLOS. It may also verify that the PDN connection has been established for the RLOS APN by querying the PCRF. This is achieved by the P-CSCF querying the PCRF. If one of the above verification fails, the SIP INVITE is rejected.

UE's IP address spoofing is still possible, but IP address spoofing is always possible for unauthenticated UEs in any solution, but proposed verifications minimize the risks as described below:

- the IP address would need to correspond to a PDN connection that corresponds to the RLOS APN.

When these verifications are performed successfully, the P-CSCF shall route the SIP request to a specific RLOS-CSCF to satisfy the IMS network isolation requirement (similar principle as for an emergency IMS session, which uses a specific E-CSCF). Emergency sessions are detected the same way as in a regular P-CSCF and, in this case, the SIP request is routed to the E-CSCF. If the P-CSCF has determined that it is an emergency call but emergency calls are not allowed over RLOS registration, the UE SIP INVITE request is rejected. If the P-CSCF has determined that it is not for an emergency service and if the RLOS-CSCF has determined that the UE SIP request if not for RLOS, the UE SIP request is rejected.

An authenticated UE in limited service state or an unauthenticated UE may request RLOS IMS services as long as it is EPC attached to the RLOS APN. Optionally, when the UE is detached from the EPC while an IMS session is still ongoing (after a timer configured for RLOS APN), the PCRF may indicate it to the P-CSCF, which shall inform RLOS-CSCF.

When provided, the network provided location information conveyed from the EPC to the P-CSCF via PCRF shall be forwarded to the RLOS-CSCF.

Charging of RLOS IMS sessions is performed by the IMS network as for a regular IMS sessions.

**P-CSCF additional features for RLOS**

- The P-CSCF can be a RLOS-specific P-CSCF or a general-purpose P-CSCF.

- The P-CSCF detects whether a SIP request from an UE is for RLOS from the RLOS indication provided by the UE. The P-CSCF may be configured with a range of IP addresses reserved for RLOS, and if so, it verifies that the UE IP address is within the range of IP addresses reserved for RLOS. It may also verify that the PDN connection is established for RLOS APN and that the IMEI/IMSI used for the EPC attach is the same as the one received in the SIP request by querying the PCRF.

- The P-CSCF selects an E-CSCF if it detects that the UE has initiated an emergency session request, according to TS 23.167 [8] clause 7.3 (Emergency Session Establishment in the Serving IMS network). The P-CSCF shall also be able to detect non-UE detectable emergency sessions as specified in TS 23.167 [8] clause 7.2.

Editor's note: Details for non UE-detectable emergency calls are FFS.

- If available, the P-CSCF shall provide RLOS-CSCF with the NPLI received from the PGW via PCRF.

- When the P-CSCF receives an indication from the PCRF that the UE has been RLOS detached from EPC while an IMS session is still active, it shall inform RLOS-CSCF.

**PCRF additional features for RLOS**

- The PCRF shall understand the RLOS indication in the request from P-CSCF asking whether the PDN connection was established for RLOS (i.e. to RLOS APN).

- When the UE is RLOS detached from the EPC, the PCRF shall indicate it to the P-CSCF.

**RLOS‑CSCF additional features for RLOS**

- Receives the RLOS indication from P‑CSCF.

- Routes RLOS session establishment requests to an appropriate destination including anonymous session establishment requests.

- Generates CDRs for RLOS.

### 7.10.2 Procedures

#### 7.10.2.1 IMS registration

The UE, when EPC attached for RLOS, skips the IMS registration the same way as in emergency session for unauthenticated UEs (See TS 23.167 [8] clause 7.1.1).

#### 7.10.2.2 Location Information retrieval

Not applicable.

#### 7.10.2.3 UE initiated RLOS IMS session establishment

The following flow contains a high-level description of the RLOS procedures.



Figure 7.10.2.3-1: UE initiated RLOS IMS session establishment

The following steps are performed:

1. The UE sends an Attach Request to the EPC including an RLOS indication. The EPC establishes a local break-out default PDN connection for RLOS to the RLOS specific APN and replies to the UE with an indication that the UE is attached for RLOS as well as with the address of a P-CSCF suitable for RLOS sessions (via PCO). The EPC also informs PCRF that the PDN connection is for RLOS. See solution #4 in the TR for details.

2. The UE skips the IMS registration.

3. If the UE requests an IMS RLOS, it sends a SIP INVITE with an RLOS indication to the P-CSCF address received in the PCO during EPC Attach. The P-CSCF, if configured with a range of IP addresses reserved for RLOS, verifies that the UE IP address is within the range of IP addresses reserved for RLOS. The P-CSCF may also query the PCRF to verify that the PDN connection is for RLOS APN and to verify that the IMSI/IMEI corresponding to the UE IP address received in the SIP INVITE is the same as the one returned by the PCRF. If one of the above verifications fails, the SIP INVITE is rejected. Otherwise, the P-CSCF verifies whether emergency calls under RLOS registration is allowed and routes the SIP INVITE to the RLOS specific CSCF. Emergency calls are detected the same way as in a regular P-CSCF, and in this case the SIP INVITE is routed to the E-CSCF.

### 7.10.3 Impact on existing entities and interfaces

UE:

- The UE shall include a RLOS indication in the SIP INVITE when requesting an IMS RLOS.

P-CSCF:

- The P-CSCF shall be able to detect the RLOS indication.

- The P-CSCF shall be able to add RLOS indication when querying PCRF, and to check if the PDN connection is for RLOS APN in the answer from PCRF.

- The P-CSCF shall be able to route the SIP requests for IMS RLOS to a specific RLOS CSCF in the local PLMN.

PCRF:

- The PCRF shall be able to store the RLOS indication provided by the PGW at IPCAN session establishment.

- The PCRF shall be able to understand the new parameter "RLOS indication" in the query from the P-CSCF and verify that the PDN connection related to the UE IP address is to the RLOS APN.

## 7.11 Solution #11: Partial security solution for key issue #EPC-7

### 7.11.1 Functional Description

NOTE: the description of this solution in this TR does not prevent work on other solutions for this key issue.

In order to reduce the fraud risks associated with RLOS, the UE shall not offer RLOS services to the user unless the serving cell has a Mobile Country Code from the set {310, …, 316}.

This does not prevent all false base station attacks outside of the USA, hence the UE should also use other sources of information (e.g. GPS, time and country of last authenticated access, etc) to warn the customer of base stations outside of the USA which are broadcasting a USA Mobile Country Code and indicating that they provide RLOS service.

### 7.11.2 Procedures

The UE does not offer RLOS service if the serving cell does not have an MCC from the set {310, …, 316}.

When the serving cell does have an MCC from the set {310, …, 316}, the UE should deploy local intelligence (e.g. based on its geographic awareness) to determine the severity of the warning it gives to any user requesting RLOS service.

### 7.11.3 Impact on existing entities and interfaces

UE:

The UE already implements special behavior for Mobile Country Codes from the set {310, …, 316}. This behavior would need to be extended to determine whether to pass RLOS information to the user.

New, implementation specific, mechanisms within the UE are needed to determine the likelihood that any cell advertising RLOS service is part of a genuine RLOS PLMN. These can be assisted by existing capabilities in the UE: e.g. the UE tracks 'time' (for periodic updating purposes) and last visited TAI (=MCC+MNC+TAC) (for part of the TAU procedure). Most modern smartphones also include GPS and potentially other GNSS capabilities.

Network:

No impact.

# 8 Evaluation

Table 8-1

|  |  |  |  |
| --- | --- | --- | --- |
| Key Issue #EPC-1: Network indicating support for Restricted Local Operator Services and related UE behaviour | Description | Advantages | Drawbacks |
| Solution #1 | 1) A new SIB provided by E-UTRAN indicates that the PLMN is configured to supports Restricted Local Operator Services.  2) The PLMNs where RLOS is supported may be stored in UICC (or ME).  3) Whether automatic PLMN selection needs to be supported for RLOS will be confirmed by CT WG1. | 1) It is the only way to prevent UEs to even send a message.  2) In line with SA WG1. | None |
| Solution #9 | 1) New SIB: same as solution #1  2) PLMN selection by user or configured in ME. | 1) Same. | 1) None for new SIB.  2) PLMN selection configured in ME would require more specification work. |

Table 8-2

|  |  |  |  |
| --- | --- | --- | --- |
| Key Issue #EPC-2: RLOS request indication | Description | Advantages | Drawbacks |
| Solution #2 | RLOS indication in Attach (UE-CN). | For entering RLOS EPC procedures. | None. |
| Solution #4 | RLOS indication in Attach (UE-CN). | For entering RLOS EPC procedures. | None. |
| Solution #9 | RLOS RRC establishment cause (UE-RAN). | For admission control in RAN. | RAN impacts. |

Table 8-3

|  |  |  |  |
| --- | --- | --- | --- |
| Key Issue #EPC-3: Support of unauthenticated UEs access to RLOS (congestion issue) | Description | Advantages | Drawbacks |
| Solution #1 | An operator may decide to unset the SIB indicator e.g. using OAM to prevent access attempts from UEs for RLOS e.g. in case of network congestion. | No impacts to the specs. | 1) RLOS for all UEs or no UEs.  2) Slow mechanism.  3) Cannot be extended to CN congestion situations. |
| Solution #9 | The E-UTRAN may reject the RRC connection establishment with extended wait timer for RLOS attempts. | 1) Per UE mechanism.  2) Fast and proportional to the level of congestion.  3) Can also apply before congestion.  4) Can be extended to CN overload by adding S1 overload message. | RAN impacts |

Table 8-4

|  |  |  |  |
| --- | --- | --- | --- |
| Key Issue #EPC-3: Support of unauthenticated UEs access to RLOS (EPC access issue) | Description | Advantages | Drawbacks |
| Solution #6 | Partial solution:  Enabling VoLTE calls after initial attachment:  - First option: the RLOS APN can lead to a portal that guides the user to various services. Alternatively, if the UE attached to RLOS APN can be IMS authenticated, the UE can use IMS APN to re-(register) in IMS.  - In the second option, the RLOS APN may lead directly to the IMS network to initiate the requested RLOS VoLTE service.  - SIP signalling may not acquire the QCI 5 that would typically be associated with an APN dedicated for IMS. | The text related to QCI=5 might not be used should be captured. | Not a full solution.  Apart from non-roamers UEs in limited service state, UEs cannot be authenticated. So, text is incorrect. |
| Solution #2 | RLOS attach with RLOS indication, no authentication, configured APN for RLOS, P-CSCF address in PCO, PGW shall block any traffic that is not from or to addresses of network entities (e.g. P-CSCF, captive portal), UE and Network shall implicitly detach without NAS signalling transactions. | Basic solution. | Some aspects are missing. |
| Solution #4 | Same as solution #2 plus charging, location services, mobility aspects.  Difference is that authentication is performed for non-roaming UEs in limited service state in order to use credentials (see key issue EPC-4). | Charging aspects, ARP aspects, PCC deployments considerations. | None. |

Table 8-5

|  |  |  |  |
| --- | --- | --- | --- |
| Key Issue #EPC-4: Support of authenticated UEs access to RLOS | Description | Advantages | Drawbacks |
| Solution #2 | UE requesting RLOS is authenticated but in limited state: MME skips the authentication. | Simple; authentication is always skipped when RLOS indication is present. | No integrity protection nor ciphering for control and user planes. |
| Solution #4 | UE requesting RLOS is authenticated and non-roamer but in limited state: MME performs the authentication to get credentials. | It allows to integrity protect and cipher control and user planes. | More complex than solution #2. |

Table 8-6

|  |  |  |  |
| --- | --- | --- | --- |
| Key Issue #EPC-6: Collection of charging information | Description | Advantages | Drawbacks |
| Solution #4 | Charging of RLOS PDN connections can be performed by OFCS and OCS as for regular PDN connections. The rating group provided by PCRF should just be a RLOS specific rating group. | No changes. Only configuration for RLOS. | None. |

Table 8-7

|  |  |  |  |
| --- | --- | --- | --- |
| Key Issue #EPC-7: Level of security | Description | Advantages | Drawbacks |
| Solution #2 | Mimics emergency calls for unauthenticated UEs per 23.617 annex K.3.  Treats all RLOS requests as for unauthenticated UEs. | The solution supports the requirement "Level of security should not be less than that which is currently applied to existing equivalent network access methods (e.g., unauthenticated emergency calling)". | Does not protect customer from false base station attacks. |
| Solution #4 | Mimics emergency calls for unauthenticated UEs per 23.617 annex K.3.  In addition, for UEs in limited service state for which subscribers belong to the local PLMN, integrity protection is ensured for signalling and ciphering is possible for control and user plane. | The solution supports the requirement "Level of security should not be less than that which is currently applied to existing equivalent network access methods (e.g., unauthenticated emergency calling)".  For UEs of the local PLMN (but which are in limited service state) it allows to integrity protect control plane and cipher the control and user planes. | Does not protect customer from false base station attacks. |
| Solution #11 | In order to reduce the fraud risks associated with RLOS, the UE shall not offer RLOS services to the user unless the serving cell has a Mobile Country Code from the set {310, ..., 316}. | Simple additional mechanism only impacting the ME to protect customer from false base station attacks. | List needs to be extended if other countries require to use RLOS. UEs need to be updated (e.g. via over the air updates).  Does not protect against fraud risks when MCC = {310, …, 316}  It relies on the UE to locate itself at "country level" that can only rely on implementation dependant methods. |

Table 8-8

|  |  |  |  |
| --- | --- | --- | --- |
| Key Issues #IMS-1: Support for unauthenticated and authenticated user  #IMS-2: Identification of Restricted Local Operator Services at IMS layer  #IMS-3: Handling IMS session for Restricted Local Operator Services | Description | Advantages | Drawbacks |
| Solution #3 | RLOS indication in SIP REGISTER.  In line with S8HR emergency calls specified in TS 23.167 [8] clause K.3.  No authentication at IMS layer since TS 23.167 [8] clause K.3 is for unauthenticated UEs. | Minimal changes if TS 23.167 [8] clause K.3 is reused as is. | No integrity protection nor ciphering for non-roaming UEs in limited service state. |
| Solution #5 | Same as solution #3 but where the non-roaming UEs in limited service state are authenticated only to retrieve credentials. | It allows to integrity protect and cipher control and user planes. | More complex than solution #3 |
| Solution #7 | In the first scenario (unauthenticated UEs), RLOS UEs are allowed to make VoLTE calls even if their IMS registration cannot be successful.  In the second scenario (authenticated UEs), RLOS UEs are registered in IMS with identities specially assigned for RLOS that allow them to make VoLTE calls. | To capture: based on operator policy, be configured with a limited set of destinations. | No clear description. Looks like solution #5 but does not state whether TS 23.167 [8] is reused or if it rely on new procedures (which would have more impacts). |
| Solution #10 | Skipping IMS registration as for emergency calls. |  | Not in line with S8HR emergency calls specified in TS 23.167 [8], clause K.3. |

Table 8-9

|  |  |  |  |
| --- | --- | --- | --- |
| Key issue #IMS-4: Support of emergency services by UEs attached for RLOS | Description | Advantages | Drawbacks |
| Solution #3 | Not described. |  |  |
| Solution #5 | UE does not detach to initiate an emergency call: the P-CSCF will route the emergency call to E-CSCF. | No need to detach from RLOS APN to obtain emergency call. Minimal changes to P-CSCF. | None. |
| Solution #8 | The UE may detach from RLOS and then do emergency Attach, or the UE may decide to stay RLOS attached and to establish an emergency PDN connectivity towards the emergency APN. |  | Not clear which procedure is intended. Complexity / more impacts if we have to implement both. |

# 9 Conclusions

For Key Issue EPC-1 (Network indicating support for Restricted Local Operator Services and related UE behaviour), it is agreed that:

- A new SIB provided by E-UTRAN indicates that the PLMN is configured to supports Restricted Local Operator Services.

- The PLMNs where RLOS is supported may be stored in UICC (or ME).

- In automatic PLMN selection, if registration cannot be achieved on any PLMN and at least one PLMN offering restricted local operator services has been found, the UE shall behave as stated in TS 22.011 [10] clause 3.2.2.2.

For Key Issue EPC-2 (RLOS request indication), it is agreed that:

- The UE shall indicate in the Attach Request that the attachment is for RLOS.

- During the RRC connection establishment procedure, the UE indicates in the RRC signalling that the RRC connection is for RLOS access, using RLOS RRC establishment cause, per solution #9.

For Key Issues EPC-3 (Support of unauthenticated UEs access to RLOS) and EPC-4 (Support of authenticated UEs access to RLOS), it is agreed that:

- For congestion issue, solution #9 is adopted.

- For EPC access issue, solution #4 is adopted with the following clarifications:

- Authentication for EPC access for roaming UEs in limited state may be performed based on local operator policy;

- MME initiated detach based on RRC release or implicit detach timer is excluded;

- Handling related to End of RLOS session is excluded (as "End of RLOS session" is not defined);

- The following PGW function proposed in solution #2 is adopted: duration of PDN connection for RLOS is controlled through local policies in PGW;

- For configuring access to IMS after initial attachment to EPC, solution #6 is adopted.

For Key Issue EPC-6 (collection of charging information), it is agreed that:

- Solution #4 is adopted.

For Key Issues IMS-1 (Support for unauthenticated and authenticated user), IMS-2 (Identification of Restricted Local Operator Services at IMS layer) and IMS-3 (Handling IMS session for Restricted Local Operator Service), it is agreed that:

- For UEs unauthenticated at IMS layer (manual roamers) and for UEs whose IMSI belongs to the local operator, the solution 7 is adopted, complemented with the solution 5 optional capabilities for security checks (to be tuned during normative phase), with the following clarification:

- Whether the P-CSCF may be configured to consider UEs whose IMSI belongs to the local operator as unauthenticated UEs will be decided by SA WG3.

For Key Issue IMS-4 (Support of emergency services by UEs attached for RLOS), it is agreed that:

- Solution in clause 7.8.2.1 "UE performs detach from RLOS and then do emergency Attach" is adopted to support emergency service for a RLOS attached UE.

For key issue EPC-7:

- In order to avoid MitM attacks, TLS can be used for any server that provides PaRLOS service e.g. using HTTPS or SIPS. How the Server authentication is performed e.g. using the server certificates and authorized trust anchor root CA certificates, procedures for validation of the server certificate, etc. will be studied in SA WG3.

- For operators that do not require support for PaRLOS they can indicate that in their terminal requirements so that PaRLOS can be by default "disabled" and enabled only after user's consent.

Overall security impacts will be further studied and concluded by SA WG3/TSG SA.

Annex <A>:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2018-09 | SP#81 | SP-180742 | - | - | - | MCC editorial update for presentation to TSG SA#81 for approval | 1.0.0 |
| 2018-09 | SP#81 | SP-180742 | - | - | - | MCC editorial update for publication after TSG SA#81 approval (correction to title to add User Equipment (UE)) | 16.0.0 |