3GPP TR 33.815 V16.0.1 (2019-10)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Security Aspects;

Study on Security Aspects of Provision of Access to Restricted Local Operator Services by Unauthenticated UEs (PARLOS)

(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

PARLOS, security

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

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

Internet

http://www.3gpp.org

***Copyright Notification***

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

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

All rights reserved.

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

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

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

Contents

Foreword [4](#__RefHeading___Toc22654913)

Introduction [5](#__RefHeading___Toc22654914)

1 Scope [6](#__RefHeading___Toc22654915)

2 References [6](#__RefHeading___Toc22654916)

3 Definitions of terms, symbols and abbreviations [6](#__RefHeading___Toc22654917)

3.1 Terms [6](#__RefHeading___Toc22654918)

3.2 Symbols [6](#__RefHeading___Toc22654919)

3.3 Abbreviations [6](#__RefHeading___Toc22654920)

4 Background [7](#__RefHeading___Toc22654921)

4.1 Summary [7](#__RefHeading___Toc22654922)

4.2 Manual roaming in operation [7](#__RefHeading___Toc22654923)

4.3 Manual roaming service [7](#__RefHeading___Toc22654924)

4.4 Manual roaming implications for RLOS [8](#__RefHeading___Toc22654925)

5 Key Issues [8](#__RefHeading___Toc22654926)

5.1 Introduction [8](#__RefHeading___Toc22654927)

5.2 Key issue #1: Establishing temporary security for PARLOS session [8](#__RefHeading___Toc22654928)

5.2.0 Introduction [8](#__RefHeading___Toc22654929)

5.2.1 Potential security threat [8](#__RefHeading___Toc22654930)

5.2.2 Potential security requirements [9](#__RefHeading___Toc22654931)

5.3 Key Issue #2: Support for Unauthenticated UEs access to RLOS using EPC [9](#__RefHeading___Toc22654932)

5.3.1 Key issue details [9](#__RefHeading___Toc22654933)

5.3.2 Potential Security threats [9](#__RefHeading___Toc22654934)

5.3.3 Potential security requirements [9](#__RefHeading___Toc22654935)

5.4 Key Issue #3: Authorization of use of PARLOS service. [9](#__RefHeading___Toc22654936)

5.4.1 Key issue details [9](#__RefHeading___Toc22654937)

5.4.2 Potential Security threats [9](#__RefHeading___Toc22654938)

5.4.3 Potential security requirements [9](#__RefHeading___Toc22654939)

5.5 Key Issue #4: User awareness of use of PARLOS service. [10](#__RefHeading___Toc22654940)

5.5.1 Key issue details [10](#__RefHeading___Toc22654941)

5.5.2 Potential Security threats [10](#__RefHeading___Toc22654942)

5.5.3 Potential security requirements [10](#__RefHeading___Toc22654943)

6 Solutions [10](#__RefHeading___Toc22654944)

6.1 Solution #1 AS and NAS security for RLOS services [10](#__RefHeading___Toc22654945)

6.1.1 Introduction [10](#__RefHeading___Toc22654946)

6.1.2 Solution details [11](#__RefHeading___Toc22654947)

6.1.2.1 PARLOS Procedure [11](#__RefHeading___Toc22654948)

6.1.2.2 Key Hierarchy for PARLOS [12](#__RefHeading___Toc22654949)

6.1.3 Evaluation [12](#__RefHeading___Toc22654950)

6.2 Solution #2 AS and NAS security based on the emergency call procedures [13](#__RefHeading___Toc22654951)

6.2.1 Introduction [13](#__RefHeading___Toc22654952)

6.2.2 Solution details [13](#__RefHeading___Toc22654953)

6.2.3 Evaluation [13](#__RefHeading___Toc22654954)

7 Conclusions [15](#__RefHeading___Toc22654955)

Annex A: Change history [16](#__RefHeading___Toc22654956)

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

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

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

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

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

**should** indicates a recommendation to do something

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

**may** indicates permission to do something

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

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# Introduction

3GPP TS 22.011 [2] defines a new service to provide Restricted Local Operator Services (RLOS) for unauthenticated UEs. The present document is a study of the security aspects of this service.

# 1 Scope

The present document will examine potential security and privacy threat scenarios enabled by PARLOS, evaluate whether solutions need to be found for these and, if required, identify security solutions and approaches which can mitigate the identified security and privacy threat scenarios while meeting the US regulatory obligations spelled out in the referenced regulations. The present document will make recommendations on the solutions considered.

The present document will consider user notification regarding security and privacy risks when using PARLOS.

The present document will consider the applicability of external security and privacy standards (e.g. Payment Card Industry Data Security Standard) to PARLOS.

# 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 22.011: "Service accessibility".

[3] 3GPP TS 22.101: "Service aspects; service principles".

[4] 3GPP TR 22.820 "Study on Provision of Access to Restricted Local Operator Services by Unauthenticated UEs; Stage 1".

[5] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

# 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

Void.

## 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].

RLOS Restricted Local Operator Service

# 4 Background

## 4.1 Summary

Work on RLOS service definition and requirements for unauthenticated UEs (PARLOS) driven primarily by US regulatory obligations to support manual roaming has been completed in [2], [3] and [4]. Meeting this US regulatory obligation add security risks and potential vulnerabilities to devices and networks supporting RLOS.

The ability to provide access to such local services has been available to U.S. operators on a proprietary basis on CS legacy networks. However, the wide deployment of LTE and corresponding introduction of VoLTE creates regulatory obligations on US operators for a standardized mechanism to allow a UE to access these services via LTE and NR (e.g., dialling a particular digit string, accessing a captive portal) without necessarily being successfully authenticated for access.

## 4.2 Manual roaming in operation

Manual roaming, an FCC obligation on US operators was first established in 1981, enhanced in 1994 and revisited without modification several times since. In summary, manual roaming is a requirement that US networks need to provide basic outbound only voice calling for users with a UE which is technically capable of connecting to a network's base stations (e.g. supporting the same bandclass), when there is no roaming agreement with the home network operator

In terms of the usage of this service in the US, some measure of the scale is over 23 million call attempts/month (276 million/year).

As a practical matter, while the US FCC regulations only applies to subscribers of US networks without domestic roaming agreements, it is currently not possible to distinguish other devices not covered by the regulation, manual roaming service is generally made available to all unauthenticated devices without distinction.

This service is also provided in Canada but the Canadian manual roaming regulatory framework has not been identified.

## 4.3 Manual roaming service

The following high-level flow describes the typical manual roaming service for most US networks' support of manual roaming.

1) The UE is unauthenticated and not registered in a US network, but is technically capable of connecting to the network's base station.

2) The user attempts to make a call.

3) The UE attempts to attach to a network as part of the call attempt but fails authentication.

4) The network verifies that the call is not an emergency call (911).

5) The network then forwards the call to the manual roaming service provider's IVR without further analysis of any signalling such as dialled digits.

6) The user interacts with the manual roaming service provider's IVR to provide financial payment information such as a prepaid account or a credit card.

7) After the financial information has been validated by the IVR, the call is placed to the desired number by the IVR (re-originated).

8) After the call is completed, the call is disconnected. If the user wants to make additional calls, the payment information needs to be re-entered.

Manual roaming only supports outbound calls, not inbound calls. This is the major difference between manual roaming and operator provided or operator supported pre-paid service.

## 4.4 Manual roaming implications for RLOS

The following list are specific aspects of manual roaming which apply to RLOS:

1) Only outbound initiated communication needs to be supported.

2) There is no need to send any 3GPP subscriber, user or device identities to the manual roaming service platform.

3) The service is on a per session or per call basis and needs to be re-established for subsequent sessions.

4) User interactions with manual roaming service IVR platform and manual roaming calling is outside the scope of RLOS. RLOS only provides the means to access the manual roaming service. In many cases the user interaction will be external to the 3GPP network.

5) Business or financial risks of providing manual roaming is outside the scope of RLOS. Rather these risks are handled by their manual roaming service platform.

Since manual roaming is a separate business and financial transaction separate from and not based on the user's subscription status with any operator, issues of IMEI blacklisting is only applicable based on RLOS operator implementation and home network operator service restrictions is not applicable. It should be noted as well, that manual roaming only provides outbound calling, a limited subset of voice services.

# 5 Key Issues

## 5.1 Introduction

This clause details the key issues identified for security aspects related to the PARLOS service. Each key issue defines the background to the issue, defines the threats related to the issue and proposes requirements that resolve the key issue.

## 5.2 Key issue #1: Establishing temporary security for PARLOS session

### 5.2.0 Introduction

When a UE requests a PARLOS connection to a PLMN, the UE may be unauthenticated or in limited service state. When the UE is in unauthenticated or in limited service state, the serving PLMN will fail to obtain credentials for the UE from the HSS and establishing regular NAS and AS context may not be possible. Without establishing the NAS and AS security context, the PLMN may not be able to secure the NAS and AS communication. Hence for UEs connecting to PARLOS portal, normal procedure for establishing NAS and AS security is not possible. Please note that, if the UE is successfully authenticated and if the network has established NAS and AS security context, the UE will not get connected to the PARLOS portal for services.

To enable services entered via PARLOS, the serving PLMN may request the user certain personal information like Name of the user, Address of the user or location of the user where service is required. For some services, the serving PLMN may request the user Credit card information to charge for the services also. Without adequate protection if these personal information is transferred, eavesdroppers will be able to overhear the communication and get hold of the personal data of the user. In many countries transfer of personal data over unprotected communication links are legally prohibited too.

Hence transfer of this personal information over unprotected communication links is a security threat in offering PARLOS services. This needs to be addressed for UEs before providing PARLOS services. A temporary security context needs to be established for UEs connecting to the PRALOS portal before PARLOS services are enabled.

### 5.2.1 Potential security threat

If the PARLOS service session is not secured, with confidentiality and integrity protection it is possible that sensitive personal data of the user, such as name, address, credit card information may be stolen by eaves-droppers.

### 5.2.2 Potential security requirements

At the minimum it shall be possible for the network and the UE to establish end to end security at the application layer while providing PARLOS services.

The UE and the MME shall integrity and confidentiality protect the NAS signalling for PARLOS services.

The UE and the eNB shall integrity and confidentiality protect the AS signalling for PARLOS services.

## 5.3 Key Issue #2: Support for Unauthenticated UEs access to RLOS using EPC

### 5.3.1 Key issue details

A large number of malicious and unauthenticated UEs with RLOS connection could deplete network resources in EPS network by incurring additional signalling and generating traffic.

### 5.3.2 Potential Security threats

The attacker can launch DoS attack on EPS network by simply introducing many malicious UEs to initiate RLOS access to the network.

### 5.3.3 Potential security requirements

## 5.4 Key Issue #3: Authorization of use of PARLOS service.

### 5.4.1 Key issue details

When a user currently attaches to a 4G or 5G network, it is clear that the serving network was authorized by the home network. However, if network authorization were to be skipped, it could enable unauthorized networks to provide service to the user. This enables the unauthorized network to become a man in the middle to any service that is being offered.

Setting up an unauthorized network is as easy as setting up a fake base station with a network in a box that broadcasts the ability to perform RLOS, while at the same time ensuring that the victims cannot attach to a real network, e.g. by jamming the existing cells. This attack would not be limited to the regions that require manual roaming but could be performed anywhere.

### 5.4.2 Potential Security threats

An unauthorized network could exploit its man in the middle position:

- The UE is required to obtain user consent for the use of PARLOS based services. If the security risks are not sufficiently explained to the user as part of this interaction, the user is likely to be unaware of the PARLOS based service security implications. The man in the middle could take advantage of this and accept the PDN session attempt and gain access to the complete communication.

- If the man in the middle is operating where the user expects to be making a manual roaming call, the man in the middle could collect payment information and other information from users.

### 5.4.3 Potential security requirements

UE shall set up RLOS sessions only with authorized networks.

NOTE: User interaction is one possible solution to user awareness.

## 5.5 Key Issue #4: User awareness of use of PARLOS service.

### 5.5.1 Key issue details

When a user currently attaches to a 4G or 5G network, the user or application on the UE can rely on the serving network to be authorized by the home network. However, if network authorization were to be skipped, it could enable unauthorized networks to provide service to the user. This enables the unauthorized network to become a man in the middle to any service that is being offered.

The user needs to be aware that different security guarantees apply, e.g. the confidentiality and integrity of the communication are not given to the same degree as in regular service usage. Furthermore, not even the serving network name can be trusted.

NOTE: Narrowband devices are not allowed to access RLOS services.

### 5.5.2 Potential Security threats

- The UE is required to obtain user consent for the use of PARLOS based services. However, the serving network name cannot be trusted. If users are not aware of existence of PARLOS services the user is likely to be unaware of the risks of using PARLOS based service. The man in the middle could take advantage of this and accept the PDN session attempt and gain access to the complete communication.

- RLOS service could be offered by a non-trustworthy network under a false name. This could damage the reputation of the network name.

### 5.5.3 Potential security requirements

UE shall not accept PARLOS service unless the service is offered by operators with a MCC present on a whitelist in the ME.

UE shall not access PARLOS service unless either of the following conditions are true:

- No USIM is present; or

- A USIM is present and the MCC of the IMSI configured in the USIM is present on a whitelist in the ME.

NOTE: User interaction is one possible solution to user awareness.

## 6 Solutions

## 6.1 Solution #1 AS and NAS security for RLOS services

### 6.1.1 Introduction

This solution addresses the AS and NAS requirements of the key issue #1 "Establishing temporary security for PARLOS session".

The ME sends an Attach request for RLOS service and then exchanges public keys with the MME in order to secure the NAS signalling. The MME generates a temporary KASME for the ME and provides it securely to the ME. Both sides continue as with a normal setup, e.g. deriving the NAS keys and AS keys as in normal mode of operation based on the temporary KASME. The MME needs the ability to generate a public/private key for securing the new NAS messages for the key exchange procedure and the MME needs to generate a temporary KASME for the ME for normal key derivation. The ME is able to generate a public/private key for securing the NAS signalling messages.

### 6.1.2 Solution details

#### 6.1.2.1 PARLOS Procedure

The ME may be preconfigured with certificates so that the MME is able to authenticate the ME in order to protect against active attacks. If the ME is not preconfigured with PARLOS credentials, then the ME generates a public key on its own, which is used together with the RLOS indication in the ATTACH request and to secure the new temporary root key KASMEtemp.



Figure 6.1.2.1-1: PARLOS security call flow

1. The ME performs PLMN selection for RLOS and perform RLOS (i.e. unauthenticated) attach to this PLMN. The ME sends a NAS ATTACH request message to the MME including an RLOS indication and the ME's Public Key KMEpub.

2. Based on the RLOS indication, the MME generates then a temporary KASMEtemp for the ME as the new master key for KNAS and KeNB.

3. The MME sends a NAS Security Mode Command to the ME with the KASMEtemp, encrypted with the ME public key.

4. This new symmetric temporary KASME is used to derive the other keys (KNAS, KeNB, KRRC) in the ME and MME for encryption and integrity protection as in normal operation. NAS encryption can be changed at this point to the newly generated KNAS.

5. The ME sends a NAS Security Mode Complete to the MME, encrypted with KNAS

6. The MME performs a bearer setup procedure for RLOS towards SGW and PGW.

7. The MME sends a AS Security Mode Command with KeNB to the eNB.

8. ME and eNB derive the AS keys KRRCenc and KRRCint as well as KUPenc.

9. The eNB sends a AS Security Mode Complete to the MME. Now ciphering on the radio interface is enabled.

10. The MME sends an ATTACH accept to the ME (secured with KNAS), the ME is now attached for RLOS.

Editor's Note: It is ffs how to address active attacks if no credentials are pre-provisioned in the ME. The system impact, especially on the ME, for certificate based authentication is ffs.

#### 6.1.2.2 Key Hierarchy for PARLOS



Figure 6.1.2.2-1: PARLOS key hierarchy

The key hierarchy for PARLOS is the same as for normal operation, only the root key KASMEtemp is generated by the MME and sent encrypted to the ME in the NAS SMC.

### 6.1.3 Evaluation

This contribution provides some proposed text from the evaluation of solution#1 of the PARLOS TR [1].

The solution relies on the UE providing a public key to the network which is used by the network to encrypt a KASME that will be used in normal way to protect the traffic between the UE and network.

The solution provides confidentiality and integrity protection for the NAS and AS signalling against passive attacks, but not against active attacks.

The first observation to make is that the proposal protects against passive attacks, i.e. if the attacker is only eavesdropping on the data between the UE and network it will not be possible for the attacker to decrypt the traffic.

Such a benefit could be gained by merely exchanging randomly generated KAMF in the clear in one of the initial messages if the attacker does not get these initial messages.

An attacker cannot force the UE to accept a RLOS call as such a call needs to be initiated by the UE.

The proposal is vulnerable to active attacks. The attacker may simply be a false base station and route RLOS call to the real network so that RLOS call setup completes successfully (note: this is necessary given that there is some authentication between the UE and RLOS server). The attacker continues to be a man-in-the- middle for the call. Alternatively, the attacker can act like a man-in-the-middle during call set-up and be aware of the KASME that is agreed by the UE and network. This would be achieved by acting like a false base station to the UE and a UE to the network. The real network would then pass the key onto the attacker's UE which could then passed onto the real UE. The attacker could then allow the rest of the call to proceed between the real UE and network as it has the keys, e.g. by getting the UE handed over to a real cell.

To minimize the time, an attacker needs to act like a false base station: an attacker passively monitors the initial messages in RLOS calls and then acts like a false base station to get the user to re-attach via the false base station after getting the call to drop.

The impact of the UE and MME of this solution are quite high in terms of the need to support public key cryptography. The gain of such an overall impact is to force the attacker to use simple man-in-the-middle active attacks as opposed to just passive attacks.

Application layer security is always possible but depends on the implementation of the service. The standardization of such application layer security for RLOS service is outside the scope of 3GPP. Due to the lack of such standardized mechanism, the security of RLOS service cannot be ensured.

## 6.2 Solution #2 AS and NAS security based on the emergency call procedures

### 6.2.1 Introduction

This solution addresses the AS and NAS requirements of the key issue #1 "Establishing temporary security for PARLOS session" and key issue #2 "Support for Unauthenticated UEs access to RLOS using EPC".

The solution uses the emergency call procedures to enable the ME to establish a connection to the RLOS server.

### 6.2.2 Solution details

The solution proposes that a RLOS call is treated similar to an unauthenticated emergency call with the following difference:

- The UE initiates an RLOS call using an appropriate user interface, by which the user chooses or is aware of the country and network the call is made on. The UE may choose to warn or restrict the RLOS calls to only countries where it is permitted by law.- The UE indicates that it wishes to make a RLOS call rather than an emergency call in the NAS signalling to the network and will only accept a RLOS call when it has initiated the call.

- The network that supports an establishment of the RLOS session connects the UE to the RLOS server rather than making a connection to the emergency service infrastructure.

Just like in an unauthenticated emergency call, the NULL ciphering and NULL integrity algorithms will be chosen as no keys are shared between the ME and network. This means that there is no protection of the user plane or signalling of the RLOS call with this solution.

It is assumed that there will be some application layer security between the ME and RLOS server.

In terms of protecting the network against DoS attack, the network could deploy similar mechanism as the one used to protect against DoS attacks with unauthenticated emergency calls, e.g. dedicated MMEs or limiting the number of simultaneous calls.

### 6.2.3 Evaluation

This solution addresses key issue #1 by establishing security contexts using the NULL algorithms and hence there is no protection of the traffic over the air at the network layer. This solution has little implementation impact as such a solution is already supported on UE and in the network (where regulatory requirements mandate the support of unauthenticated emergency calls). RLOS calls using this solution is already deployed in some countries, where it is mandated to support.

The establishment of an RLOS call may be unauthenticated, and in such a case, it is not possible for the UE to authenticate the network. Even though the RLOS call is always initiated by the UE, an attacker may use application layer interactions to trick the user into initiating an RLOS call to a network under attacker's control. Note that such application layer attacks could be possible even if the UE is able to authenticate the network (e.g., an attacker can trick the user to make a call to the attacker and act as a man-in-the middle for the call). Such application layer attacks cannot be protected at the 3GPP network layer.

Application layer security for RLOS is always possible but depends on the implementation of the service. The standardization of such application layer security for RLOS service is outside the scope of 3GPP. Due to the lack of such standardized mechanism, the security of RLOS service cannot be ensured.

The solution addresses key issue #2 by using existing techniques on the network to prevent DoS attacks (such techniques needs to deal with cases of unprotected connections to the 3GPP network where the regulatory requirements mandate the support of unauthenticated emergency calls).

6.3 Solution #3 Network Authorization in RLOS

6.3.1 Introduction

This solution provides enhancements needed for Solution #2 (AS and NAS security based on the emergency call procedures) to address key issue # 3 (Authorization of use of PARLOS service) and key issue #4 (User awareness of use of PARLOS service).

6.3.2 Solution details

In this solution, Solution #2 is enhanced with UE based mechanisms to protect against the fact that there is no authentication of the network for RLOS connection. A UE that supports RLOS shall implement the following mechanisms:

1) Only certain applications (e.g., phone application) on the ME need to trigger establishment of RLOS connection. The ME shall enforce access control on applications that are authorized to trigger establishment of RLOS connection. Applications on the ME that are not explicitly authorized (e.g., messaging app) shall not be allowed to trigger establishment of RLOS connection.

2) A user confirmation shall be requested before the ME triggers RLOS connection establishment procedures. As part of the user confirmation, the user shall be warned of the security risk due to the lack of lack of network authentication in solution #2.

3) An attacker may spoof the network name of an operator who is not required to provide RLOS service or advertise RLOS service. This attack is mitigated by requiring the ME to maintain a white list of MCCs where RLOS is supported. The ME shall check that the MCC of the network name that advertises RLOS service is present in the white list before initiating RLOS connection.

4) An operator who is not required to provide RLOS service may want to protect their subscribers (i.e., ones with a valid USIM) against a man-in-the middle attack, where the attacker forces the UE into limited service state and tricks the users into triggering an RLOS connection. This attack is mitigated by requiring that the ME check that the MCC of the IMSI configured in the USIM is in the whitelist. If a valid USIM is present, the ME shall check that the MCC part of the IMSI configured in the USIM is present in the whitelist before initiating RLOS connection.

6.3.3 Evaluation

Requiring the UE to enforce access control on applications (Enhancement #1) protects against the threat of an attacker using application layer interactions to trick the user into making an RLOS connection.

Mandating user confirmation, along with the warning of security risk before establishment of each RLOS connection (Enhancement #2) ensures that the user is made aware of the security risks of using RLOS.

Requiring the UE to maintain a white list of MCCs where RLOS is supported and verify that the MCC of the network that advertises RLOS is present in the white list (Enhancement #3) ensures that an attacker cannot use the network name of an operator from a country where RLOS is not used.

Requiring that the ME check that the MCC of the IMSI configured on the USIM is present in the whitelist (Enhancement #4) protects an operator subscriber against a man-in-the middle attack where the attacker forces the UE into limited service state and tricks the user into triggering an RLOS connection.

# 7 Conclusions

It is clear that support of RLOS increases the security risks for the PLMNs which choose to support it as demonstrated by the limited strength of the solutions contained in this specification to address the various potential security threats identified in this specification. Some operators may have regulatory obligations to support RLOS which may limit the range of implementation choices that they are able to consider. Other operators who have the option not to support RLOS likewise have concerns of limiting RLOS in their networks, even limiting UE initiation of RLOS requests in their PLMN.

This study has identified that an approach which identifies RLOS calls from unauthenticated UEs in a fashion similar to emergency call procedures (solution #2 described above) is the only practical approach available, allows for reuse of some emergency call procedures related to unauthenticated UEs. However, emergency calls for unauthenticated UEs only support a very limited set of capabilities to deal with security risks identified in this study.

In the light of this, additional capabilities associated with RLOS have been identified in this study which allow further restrictions of the use of RLOS to PLMNs supporting RLOS while limiting even the initiation of PARLOS service requests in PLMNs not supporting RLOS as identified in solution #3. Therefore, it is concluded that solution #3 is chosen as the way forward for normative work as a new Annex in TS 33.401 [5].

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2019-09 | SA#85 | SP-190690 |  |  |  | Presented for information and approval | 1.0.0 |
| 2019-09 | SA#85 | SP-190887 |  |  |  | Revised to include the right version of the draft | 1.0.1 |
| 2019-09 | SA#85 |  |  |  |  | Change control version | 16.0.0 |
| 2019-10 |  |  |  |  |  | EditHelp review | 16.0.1 |