3GPP TR 33.856 V16.1.0 (2019-06)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Study on security aspects of single radio voice continuity from 5G to UTRAN

(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

Security,5G,UTRAN,SRVCC

***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 5](#__RefHeading___Toc530492376)

[Introduction 5](#__RefHeading___Toc530492377)

[1 Scope 6](#__RefHeading___Toc530492378)

[2 References 6](#__RefHeading___Toc530492379)

[3 Definitions and abbreviations 6](#__RefHeading___Toc530492380)

[3.1 Definitions 6](#__RefHeading___Toc530492381)

[3.2 Abbreviations 6](#__RefHeading___Toc530492382)

[4 Overview 6](#__RefHeading___Toc530492383)

[5 Key issues 7](#__RefHeading___Toc530492384)

[5.1 Key Issue #1: Achieving backward security of key derivation during SRVCC from 5G to UTRAN CS 7](#__RefHeading___Toc530492385)

[5.1.1 Key issue details 7](#__RefHeading___Toc530492386)

[5.1.2 Security threats 7](#__RefHeading___Toc530492387)

[5.1.3 Potential Security requirements 7](#__RefHeading___Toc530492388)

[5.2 Key Issue #2: Security of IMS Emergency Session Handling 7](#__RefHeading___Toc530492389)

[5.2.1 Key issue details 7](#__RefHeading___Toc530492390)

[5.2.2 Security threats 7](#__RefHeading___Toc530492391)

[5.2.3 Potential Security requirements 8](#__RefHeading___Toc530492392)

[5.3 Key Issue #3: Protecting the SRVCC capability 8](#__RefHeading___Toc530492393)

[5.3.1 Key issue details 8](#__RefHeading___Toc530492394)

[5.3.2 Security threats 8](#__RefHeading___Toc530492395)

[5.3.3 Potential Security requirements 8](#__RefHeading___Toc530492396)

[5.4 Key Issue #4: 5G UE returning from 3G SRVCC to E-UTRA or NR 8](#__RefHeading___Toc530492397)

[5.4.1 Key issue details 8](#__RefHeading___Toc530492398)

[5.4.2 Security threats 8](#__RefHeading___Toc530492399)

[5.4.3 Potential Security requirements 8](#__RefHeading___Toc530492400)

[6 Solutions 9](#__RefHeading___Toc530492401)

[6.1 Solution #1.1: Key derivation during SRVCC from 5G to UTRAN CS without direct interface between AMF and MSC server 9](#__RefHeading___Toc530492402)

[6.1.1 Introduction 9](#__RefHeading___Toc530492403)

[6.1.2 Solution details 9](#__RefHeading___Toc530492404)

[6.1.3 Impacts on existing nodes and functionality 10](#__RefHeading___Toc530492405)

[6.1.4 Evaluation 10](#__RefHeading___Toc530492406)

[6.2 Solution #1.2: Key derivation during SRVCC from 5G to UTRAN CS with direct interface between AMF and MSC server 10](#__RefHeading___Toc530492407)

[6.2.1 Introduction 10](#__RefHeading___Toc530492408)

[6.2.2 Solution details 11](#__RefHeading___Toc530492409)

[6.2.3 Impacts on existing nodes and functionality 11](#__RefHeading___Toc530492410)

[6.2.4 Evaluation 12](#__RefHeading___Toc530492411)

[6.3 Solution #2: Emergency session in SRVCC from 5G to UTRAN CS 12](#__RefHeading___Toc530492412)

[6.3.1 Introduction 12](#__RefHeading___Toc530492413)

[6.3.2 Solution details 12](#__RefHeading___Toc530492414)

[6.3.3 Impacts on existing nodes and functionality 12](#__RefHeading___Toc530492415)

[6.3.4 Evaluation 12](#__RefHeading___Toc530492416)

[6.4 Solution #3: Protecting the SRVCC capability 12](#__RefHeading___Toc530492417)

[6.4.1 Introduction 12](#__RefHeading___Toc530492418)

[6.4.2 Solution details 13](#__RefHeading___Toc530492419)

[6.4.3 Impacts on existing nodes and functionality 13](#__RefHeading___Toc530492420)

[6.4.4 Evaluation 13](#__RefHeading___Toc530492421)

[6.5 Solution #4: Return from UTRAN to E-UTRAN or NR 13](#__RefHeading___Toc530492422)

[6.5.1 Introduction 13](#__RefHeading___Toc530492423)

[6.5.2 Solution details 13](#__RefHeading___Toc530492424)

[6.5.3 Impacts on existing nodes and functionality 13](#__RefHeading___Toc530492425)

[6.5.4 Evaluation 13](#__RefHeading___Toc530492426)

[7 Conclusions 14](#__RefHeading___Toc530492427)

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

# Introduction

The interworking between NR and UTRAN is not supported in 3GPP, leading to the lack of Voice Call Continuity from NR to UTRAN. This may cause problem to voice service, when NR coverage is limited, as listed below:

Scenario # – Operators with both VoNR and VoLTE enabled:

- In the initial stage of 5G deployment, the voice service continuity may not be guaranteed if the VoLTE coverage provided by the operators is not (ideal) complete, i.e., there are some "holes" of VoLTE coverage.

The present document presents the security aspects of single radio voice continuity from 5G to UTRAN.

# 1 Scope

The present document studies the security aspects of single radio voice continuity from 5G to UTRAN CS. In particular, the goal of the present document is to study the impacts on 3GPP security architecture which may result from 5GS to UTRAN CS voice continuity, e.g. security context mapping from 5G and UTRAN, security procedure for the emergency call, etc.

# 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 TS 33.501: "Security architecture and procedures for 5G system".

[2] 3GPP TR 23.756: Study for single radio voice continuity from 5G to 3G".

[3] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[4] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[5] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC)".

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [3] 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 [3].

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [3] 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 [3].

AMF Access and Mobility Management Function

CS Circuit Switched

EPS Evolved Packet System

E-UTRAN Evolved UTRAN

HO HandOver

IMS IP Multimedia Subsystem

MSC Mobile Switching Center

NAS Non Access Stratum

NR New Radio

PS Packet Switched

SRVCC Single Radio Voice Call Continuity

UE User Equipment

UMTS Universal Mobile Telecommunications System

UTRAN Universal Terrestrial Radio Access Network

# 4 Overview

The interworking between NR and UTRAN is not supported in 3GPP, leading to the lack of Voice Call Continuity from NR to UTRAN. This may cause problem to voice service, have impact on the user experience, when NR coverage is limited, as listed below:

Scenario #1 – Operator with both VoNR and VoLTE enabled

- In the initial stage of 5G deployment, the voice service continuity may not be guaranteed if the VoLTE coverage provided by the operators is not (ideal) complete, i.e., there are some “holes” of VoLTE coverage.

Scenario #2 – Operator with both VoNR and LTE enabled, but no VoLTE

- Some operators deploys VoNR and LTE, but do not launch VoLTE in their LTE network, which means VoNR will be dropped if the UE moves from 5G coverage to LTE coverage.

Scenario #3 – Operator with VoNR but no LTE (nor VoLTE)

- In some countries, the operators only have GSM/UTRAN deployment currently. Deploying 5G system and VoNR directly would be infeasible for them since the voice continuity cannot be guaranteed. Thus the voice service continuity from 5G to UTRAN is supported for MNOs that are in one of the above scenarios, in order to enable such an MNO to offer a good service to its subscribers.

# Thus, the security related analysis for the requirements identified in TS 23.216 [5] and candidate solutions of supporting single radio voice continuity from 5GS to UTRAN CS is necesary.5 Key issues

## 5.1 Key Issue #1: Achieving backward security of key derivation during SRVCC from 5G to UTRAN CS

### 5.1.1 Key issue details

During SRVCC from 5G to UTRAN CS, the MSC server should never know the KAMF nor should the KAMF be revealed to an entity other than AN AMF. If the AMF or the MME does not derive new key(s) to create a mapped SRVCC security context for the MSC server instead of sending KAMF to the MSC server, or if the keys sent to the MSC server are not generated properly, the MSC server or an attacker can gain knowledge of KAMF and violate backward security.

### 5.1.2 Security threats

If the backward security is not achieved, the key received from the AMF may be used to attack 5G system, for example, deriving other keys based on KAMF and recover communication between a UE and the system.

### 5.1.3 Potential Security requirements

- backward security shall be achieved when handover is performed from the AMF to the MSC server.

## 5.2 Key Issue #2: Security of IMS Emergency Session Handling

### 5.2.1 Key issue details

During SRVCC from 5G to 3G, IMS Emergency Sessions can be made by:

- normally attached UEs; or

- UEs attached for emergency bearer services.

IMS Emergency Services can be authenticated or unauthenticated, it depends on the serving network policy if unauthenticated IMS Emergency Sessions are allowed. Any behaviour not explicitly specified as being special to IMS Emergency Sessions is handled in accordance to normal procedures.

If the SRVCC is for an emergency call, the UE is not in limited service state, it initiates normal initial attach when not already attached to receive emergency bearer services. If the serving network attempts to authenticate the UE after receiving a request for emergency bearer services which was integrity protected by the current NAS security context and the authentication failed and if the serving network policy does not allow unauthenticated IMS Emergency Sessions, the UE and AMF proceed as for set up of normal bearers.

In this scenario, since the serving network policy does not allow unauthenticated IMS Emergency Sessions, the continuous authentication process may exhaust UE and network resource.

### 5.2.2 Security threats

If the serving network policy does not allow unauthenticated IMS Emergency Sessions, the continuous authentication process may exhaust the resources of UE and network.

### 5.2.3 Potential Security requirements

The continuous authentication process during the IMS Emergency Session handling shall be avoided.

## 5.3 Key Issue #3: Protecting the SRVCC capability

### 5.3.1 Key issue details

To support 5G-SRVCC, SRVCC Capability, MS Classmark 2 and Supported Codecs IE are sent to the AMF by the UE via initial Registration Request message, non-periodic Registration message, and by a source AMF to a target AMF during Intra-5GS handover.

### 5.3.2 Security threats

If the UE SRVCC capability sent to the network or between AMFs is tampered with, the network may not be able to provide SRVCC service to the user and the user's call will be dropped when UE leaves 5G service area and enters into UMTS coverage. This leads to bad user experience and denial of service.

### 5.3.3 Potential Security requirements

UE SRVCC Capability, MS Classmark 2 and Supported Codecs IE should be protected from modification when sent in the initial Registration message, non-periodic Registration or sent between source AMF and target AMF.

## 5.4 Key Issue #4: 5G UE returning from 3G SRVCC to E-UTRA or NR

### 5.4.1 Key issue details

A 5G UE that is handed off to 3G SRVCC is not allowed to return to either E-UTRA or NR without explicit (re)authentication after the CS voice call is released, regardless of whether the UE has a valid EPS security context or a NR security context.

### 5.4.2 Security threats

When a voice service ends in UTRAN and NR coverage is not available, the UE may use current security context (UMTS) to derive a mapped EPS security context as described in subclause 9.1.2 of TS 33.401 [4].In this case, the UE may potentially get back to NR with a security context that is based on 3G. If this is allowed, once the NR coverage is available, the UE will return to NR by executing the procedures as described in subclause 8.2 or 8.4 of TS 33.501 [1], however, the context will have been derived from the UMTS session.

Using UMTS security context to derive a mapped EPS security context including the subsequent 5GS security context will jeopardize 5G security due to the lower security level of UMTS potentially leading to far more serious attacks in the network.

### 5.4.3 Potential Security requirements

- A UE that is handed off to 3G SRVCC shall be prohibited to return to E-UTRAN and NR without explicit (re)authentication if NR coverage is not available.

- The network shall prohibit a UE that is handed off to 3G SRVCC shall be prohibited from returning to E-UTRAN and NR without explicit (re)authentication if NR coverage is not available.

# 6 Solutions

## 6.1 Solution #1.1: Key derivation during SRVCC from 5G to UTRAN CS without direct interface between AMF and MSC server

### 6.1.1 Introduction

This solution addresses the key issue #1, namely achieving backward security of key derivation during SRVCC from 5G to UTRAN CS if there is no direct interface between the AMF and the MSC server.

### 6.1.2 Solution details



Figure 6.1.2: Key derivation of 5G to UTRAN CS during SRVCC without direct interface between AMF and MSC server

1. The gNB sends Handover Required message to the AMF.

2. The AMF derives a new K'ASME key using the KAMF key and the current downlink 5G NAS COUNT of the current 5G security context similar to as described in clause 8.6.1 of TS 33.501 [1]. A new FC value may be used..

3. The AMF assigns the value of ngKSI to the eKSI (maps ngKSI to eKSI) and transfers the new K'ASME key and the UE security capability to the MME via PS to CS HO request message.

4. The MME may further derive the CKSRVCC, IKSRVCC based on the new K'ASME key, or treat the received new K'ASME key as the concatenation of the CKSRVCC, IKSRVCC. Then the MME assigns the value of eKSI to KSISRVCC (maps eKSI to KSISRVCC) and transfers CKSRVCC, IKSRVCC with KSISRVCC, downlink 5G NAS COUNT and the UE security capability to the MSC server in PS to CS HO request message.

NOTE: MME and UE need to agree on how CKSRVCC, IKSRVCC are derived (e.g. via a new key generation procedure using K'ASME or treating K'ASME as a simple concatenation of CKSRVCC, IKSRVCC). If a new FC value is not used, a new key needs to be derived.

5. The MSC server sends the PS to CS HO response message to the MME.

6. The MME sends the Forward relocationHO response message including the security parameters in step 4 to the AMF.

7. The AMF sends the HO command to the gNB, in which includes the security parameters in step 6.

8. The gNB sends the HO command to the UE, in which includes the security parameters in step 7.

9. When the UE receives the message, it derives the new K'ASME key using the KAMF key and the current downlink 5G NAS COUNT, and identifies the CKSRVCC and IKSRVCC as the MME does.

If the SRVCC handover is not completed successfully, the new mapped CKSRVCC, IKSRVCC and KSISRVCC cannot be used. The MSC server enhanced for SRVCC deletes the newly mapped SRVCC security context for the UE, including CKSRVCC, IKSRVCC and KSISRVCC.

### 6.1.3 Impacts on existing nodes and functionality

MME:

- It needs to derive CK||IK from received K'ASME according to "SRVCC HO Indication" received from AMF.

UE:

- It needs to derive CK||IK from K'ASME which are derived from KAMF.

### 6.1.4 Evaluation

For Key Issue# 1: Achieving backward security of key derivation during SRVCC from 5G to UTRAN CS:

- Solution#1.1 is used in the scenario that no direct interface exists between the AMF and the MSC server:

- For the AMF, a new K'ASME key needs to derive, the downlink 5G NAS COUNT is reused.

- For the MME, the CK and IK for SRVCC based on the new K'ASME key need to derive.

- For the UE, a new K'ASME key need to derive, the downlink 5G NAS COUNT is reused.

TR 23.756 [2] has decided to reuse the existing SRVCC mechanism as much as possible to minimize the impact on 5GS and UMTS, it is therefore there is no direct interface between AMF and MSC server. This solution for key issue #1 describes the key derivation during SRVCC from 5G to UTRAN CS via MME.

This solution reuses the current parameters of 5G security context as much as possible, and can minimize the impact on 5GS and UTRAN.

## 6.2 Solution #1.2: Key derivation during SRVCC from 5G to UTRAN CS with direct interface between AMF and MSC server

### 6.2.1 Introduction

This solution addresses the key issue #1, namely achieving backward security of key derivation during SRVCC from 5G to UTRAN CS if there is a direct interface between the AMF and the MSC server.

### 6.2.2 Solution details



Figure 6.2.2: Key derivation of 5G to UTRAN CS during SRVCC with direct interface between AMF and MSC server

1. The gNB sends Handover Required message to the AMF.

2. The AMF derives CKSRVCC||IKSRVCC using the KAMF key and the current downlink 5G NAS COUNT of the current 5G security context.

3. The AMF assigns the value of ngKSI to the KSISRVCC (maps ngKSI to KSISRVCC) and transfers the CKSRVCC||IKSRVCC and the UE security capability to the MSC server via PS to CS HO request message.

4. The MSC server sends the PS to CS HO response message to the AMF.

5. The AMF sends the HO command to the gNB, in which includes the security parameters in step 3.

6. The gNB sends the HO command to the UE, in which includes the security parameters in step 5.

7. When the UE receives the message, it derives the CKSRVCC||IKSRVCC using the KAMF key and the current downlink 5G NAS COUNT.

If the SRVCC handover is not completed successfully, the new mapped CKSRVCC, IKSRVCC and KSISRVCC cannot be used. The MSC server enhanced for SRVCC deletes the newly mapped UE SRVCC security context, including CKSRVCC, IKSRVCC and KSISRVCC.

### 6.2.3 Impacts on existing nodes and functionality

AMF:

- AMF needs to derive CK||IK directly from received KAMF according to "SRVCC HO Indication" received from gNB.

UE:

- UE needs to derive CK||IK directly from KAMF.

### 6.2.4 Evaluation

For Key Issue# 1: Achieving backward security of key derivation during SRVCC from 5G to UTRAN CS:

- Solution#1.2 is used in the scenario that there is a direct interface between the AMF and the MSC server:

- For the AMF, the CK and IKfor SRVCC is derived by using the KAMF key, the downlink 5G NAS COUNT of the current 5G security context is reused.

- For the UE, the CK and IKfor SRVCC is derived by using the KAMF key, the downlink 5G NAS COUNT of the current 5G security context is reused.

This solution reuses the current parameters of 5G security context as much as possible.

## 6.3 Solution #2: Emergency session in SRVCC from 5G to UTRAN CS

### 6.3.1 Introduction

This clause addresses the key issue #2 for authenticated emergency session and unauthenticated emergency session.

### 6.3.2 Solution details

When the SVRCC is for an authenticated emergency session or an unauthenticated emergency session, the security procedure in solution #1.1 is applied if there is no direct interface between the AMF and the MSC server. Otherwise if there is direct interface between the AMF and the MSC server, the security procedure in solution #1.2 is applied.

In the case when the SRVCC is for an unauthenticated emergency session, since the derived keys have no ability to affect the output of the NULL algorithms, However, call set up needs to continue even though the network and the UE derive different keys.

### 6.3.3 Impacts on existing nodes and functionality

In case there is no direct interface between the AMF and the MSC server, subclause 6.1.3 in the present document applies.

In case there is direct interface between the AMF and the MSC server, subclause 6.2.3 in the present document applies.

### 6.3.4 Evaluation

This solution applies the security procedure in solution #1.1 or solution #1.2, it can avoid the continuous authentication process during the IMS Emergency Session handling in SRVCC from 5G to UTRAN CS.

The details of evaluation for solution #1.1and solution #1.2 can be seen in clause 6.1.3 and 6.2.3.

This solution satisfies the requirement of key issue#2. . For an authenticated emergency session, the security procedure in subclause 6.1.3 or 6.2.3 is applied. For an unauthenticated emergency session, call set up needs to continue even when the network and the UE derive different key.

## 6.4 Solution #3: Protecting the SRVCC capability

### 6.4.1 Introduction

This solution addresses the key issue #3, namely protecting the SRVCC capability.

### 6.4.2 Solution details

For protecting the SRVCC capability in conjunction with the MS Classmark 2 and Supported Codecs IE in initial Registration Request message, the hash based method specified in subclause 6.7.2 in TS 33.501 [1] can be reused to address the problem.

For protecting the SRVCC capability in Intra-5G handover procedure, the messages between source AMF and target AMF are protected by NDS/IP.

### 6.4.3 Impacts on existing nodes and functionality

There is no impact on the existing UTRAN and EPS system.

### 6.4.4 Evaluation

TR 23.756 [2] has decided to reuse the existing SRVCC mechanism to send the SRVCC capability, MS Classmark 2 and Supported Codecs IE in an initial Registration Request message and in the Intra-5G handover procedure.

## 6.5 Solution #4: Return from UTRAN to E-UTRAN or NR

### 6.5.1 Introduction

This solution addresses the key issue #4, namely return from UTRAN to E-UTRAN or NR.

### 6.5.2 Solution details

When a voice service ends in UTRAN and NR coverage is available, if the native 5G security context stored on the UE is available, it should be used for protecting the Registration Request message. If the native 5G security context is not available (even if a mapped 5G security context is available), the AMF performs a(n) (re-) authentication procedure with the UE to establish a new native 5G security context.

When there is no NR coverage but E-UTRAN is available, if the native 5G security context stored on the UE is available, the UE deletes the UMTS security context and set the native 5G security context to current security context when receives the RRC release message from UTRAN. Then the UE should return to E-UTRAN by sending a TAU request message to the MME which is integrity protected using current native 5G security context as described in subclause 8.5 of TS 33.501 [1]. If the native 5G security context is not available (even if a mapped 5G security context is available), the MME performs a(n) (re-)authentication procedure with the UE to establish a new native EPS security context.

### 6.5.3 Impacts on existing nodes and functionality

There is no impact on the existing UTRAN, EPS, and 5GS.

UE:

- It needs to delete the UMTS security context and set the stored non-current native 5G security context to the current one when receives the RRC release message from UTRAN.

AMF:

- It needs to perform a(n) (re-)authentication procedure with the UE to establish a new native 5G security context, in case that the native 5G security context is not available when a voice service ends in UTRAN and NR coverage is available.

### 6.5.4 Evaluation

This solution satisfies the requirement of key issue #4.

- This solution prevents UE from using lower security level based on UMTS to access E-UTRAN or NR.

# 7 Conclusions

**Conclusion for Key Issue#1: Achieving backward security of key derivation during SRVCC from 5G to UTRAN CS:**

TR 23.756 reuses the existing SRVCC mechanism as much as possible and can minimize the impact on 5GS and UTRAN, therefore the solution #1.1 is selected as the basis for normative work to resolve key issue#1.

Normative work is expected to be reflected in TS 33.501 [1] for this aspect.

**Conclusion for Key Issue#2:** Security of IMS Emergency Session Handling:

Solution#2 is selected as the basis for normative work to resolve key issue#2: Security of IMS Emergency Session Handling.

Normative work is expected to be reflected in TS 33.501 [1] for this aspect.

**Conclusion for Key Issue#3:** Protecting the SRVCC capability:

Solution #3 is selected to resolve key issue #3 (Protecting the SRVCC capability), and it is expected to be the basis of normative work. Since messages between AMFs during Intra-5G handover are protected using NDS/IP, the security issue related protecting UE SRVCC capability has been addressed and no further normative work is expected.

As solution #1 contains proper key separation for SRVCC handover from 5G to UMTS CS and the introduction of this feature does not include a new way to return to 5G, the introduction of this feature does not weaken the 5G security of operators who do not deploy SRVCC handovers from 5G to UMTS CS.

**Conclusion for Key Issue#4: 5G UE returning from 3G SRVCC to E-UTRA or NR:**

Solution#4 is selected as the basis for normative work to resolve key issue#4: 5G UE returning from 3G SRVCC to E-UTRA or NR.

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2018-12 | SA#82 | SP-181032 |  |  |  | EditHelp and MCC revision. Presented for approval | 2.0.0 |
| 2018-12 | SA#82 |  |  |  |  | Upgrade to change control version | 16.0.0 |
| 2019-06 | SA#84 | SP-190360 | 0001 | 1 | F | Overview of TR33.856 | 16.1.0 |
| 2019-06 | SA#84 | SP-190360 | 0002 | - | F | Content of clause 3 for TR33.856 | 16.1.0 |