|  |  |
| --- | --- |
| 3GPP TR 33.853 V1.1.0 (2020-08) | |
| Technical Specification | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Key issues and potential solutions for integrity protection of the user plane;  (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 Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword [6](#__RefHeading___Toc42274263)

Introduction [7](#__RefHeading___Toc42274264)

1 Scope [8](#__RefHeading___Toc42274265)

2 References [8](#__RefHeading___Toc42274266)

3 Definitions of terms, symbols and abbreviations [9](#__RefHeading___Toc42274267)

3.1 Terms [9](#__RefHeading___Toc42274268)

3.2 Symbols [9](#__RefHeading___Toc42274269)

3.3 Abbreviations [9](#__RefHeading___Toc42274270)

4 3GPP Network Options [9](#__RefHeading___Toc42274271)

5 Key Issues [9](#__RefHeading___Toc42274272)

5.1 Key Issue 1: UP integrity activation in EPS [9](#__RefHeading___Toc42274273)

5.1.1 Issue description [9](#__RefHeading___Toc42274274)

5.1.2 Network options affected [10](#__RefHeading___Toc42274275)

5.1.3 Threat description [10](#__RefHeading___Toc42274276)

5.1.4 Potential security requirements [10](#__RefHeading___Toc42274277)

5.2 Key Issue #2: Secure negotiation of integrity protection support in EPS [10](#__RefHeading___Toc42274278)

5.2.1 Issue description [10](#__RefHeading___Toc42274279)

5.2.2 Network options affected [10](#__RefHeading___Toc42274280)

5.2.3 Threat description [10](#__RefHeading___Toc42274281)

5.2.4 Potential security requirements [10](#__RefHeading___Toc42274282)

5.3 Key Issue 3: UE support of UP IP at the full uplink data rate [11](#__RefHeading___Toc42274283)

5.3.1 Issue description [11](#__RefHeading___Toc42274284)

5.3.2 Network options affected [11](#__RefHeading___Toc42274285)

5.3.3 Threat description [11](#__RefHeading___Toc42274286)

5.3.4 Potential security requirements [11](#__RefHeading___Toc42274287)

5.4 Key Issue 4: Integrity protection capability imbalance in enodeB connected to 5GC [11](#__RefHeading___Toc42274288)

5.4.1 Issue description [11](#__RefHeading___Toc42274289)

5.4.2 Network options affected [12](#__RefHeading___Toc42274290)

5.4.3 Threat description [12](#__RefHeading___Toc42274291)

5.4.4 Potential security requirements [12](#__RefHeading___Toc42274292)

5.5 Key Issue 5: Optionality of integrity protection in UP DRB with 5GC [13](#__RefHeading___Toc42274293)

5.5.1 Issue description [13](#__RefHeading___Toc42274294)

5.5.2 Network options affected [13](#__RefHeading___Toc42274295)

5.5.3 Threat description [13](#__RefHeading___Toc42274296)

5.5.4 Potential security requirements [13](#__RefHeading___Toc42274297)

5.6 Key Issue 6: UE connected to 5GC indicating support of UP IP over eUTRA [14](#__RefHeading___Toc42274298)

5.6.1 Issue description [14](#__RefHeading___Toc42274299)

5.6.2 Network options affected [14](#__RefHeading___Toc42274300)

5.6.3 Threat description [14](#__RefHeading___Toc42274301)

5.6.4 Potential security requirements [14](#__RefHeading___Toc42274302)

5.8 Key Issue 8: HPLMN Control of UP IP usage in EPC5.X.1 Issue description [15](#__RefHeading___Toc42274303)

5.8.1 [15](#__RefHeading___Toc42274304)

5.8.2 Network options affected [15](#__RefHeading___Toc42274305)

5.8.3 Threat description [15](#__RefHeading___Toc42274306)

5.8.4 Potential security requirements [15](#__RefHeading___Toc42274307)

5.x Key Issue x: <Key Issue Title> [15](#__RefHeading___Toc42274308)

5.x.1 Issue description [15](#__RefHeading___Toc42274309)

5.x.2 Network options affected [15](#__RefHeading___Toc42274310)

5.x.3 Threat description [16](#__RefHeading___Toc42274311)

5.x.4 Security requirements [16](#__RefHeading___Toc42274312)

6 Potential Solutions [16](#__RefHeading___Toc42274313)

6.1 Solution #1: Dedicated PDU for UP Signalling message IP [16](#__RefHeading___Toc42274314)

6.1.1 Introduction [16](#__RefHeading___Toc42274315)

6.1.2 Network options affected [16](#__RefHeading___Toc42274316)

6.1.3 Solution Description [16](#__RefHeading___Toc42274317)

6.1.4 Solution evaluation [17](#__RefHeading___Toc42274318)

6.2 Solution #2: Integrity protection between SgNB and UE in NGEN-DC [17](#__RefHeading___Toc42274319)

6.2.1 Introduction [17](#__RefHeading___Toc42274320)

6.2.2 Network options affected [17](#__RefHeading___Toc42274321)

6.2.3 Solution description [18](#__RefHeading___Toc42274322)

6.2.4 Solution Evaluation [18](#__RefHeading___Toc42274323)

6.3 Solution #3: Improved MR-DC bearer handling [18](#__RefHeading___Toc42274324)

6.3.1 Introduction [18](#__RefHeading___Toc42274325)

6.3.2 Network options affected [18](#__RefHeading___Toc42274326)

6.3.3 Solution Description [18](#__RefHeading___Toc42274327)

6.3.4 Solution evaluation [19](#__RefHeading___Toc42274328)

6.4 Solution #4: Zero-overhead user plane integrity protection on the link layer [20](#__RefHeading___Toc42274329)

6.4.1 Introduction [20](#__RefHeading___Toc42274330)

6.4.2 Network options affected [21](#__RefHeading___Toc42274331)

6.4.3 Solution description [21](#__RefHeading___Toc42274332)

6.4.4 Solution Evaluation [24](#__RefHeading___Toc42274333)

6.5 Solution #5: Integrity Protection of packet header in the User Plane [25](#__RefHeading___Toc42274334)

6.5.1 Introduction [25](#__RefHeading___Toc42274335)

6.5.2 Network options affected [25](#__RefHeading___Toc42274336)

6.5.3 Solution Description [25](#__RefHeading___Toc42274337)

6.5.4 Solution Evaluation [26](#__RefHeading___Toc42274338)

6.6 Solution #6: Addition of UP IP for eUTRA with 5GC [26](#__RefHeading___Toc42274339)

6.6.1 Introduction [26](#__RefHeading___Toc42274340)

6.6.2 Network options affected [26](#__RefHeading___Toc42274341)

6.6.3 Solution Description [27](#__RefHeading___Toc42274342)

6.6.4 Solution Evaluation [27](#__RefHeading___Toc42274343)

6.7 Solution #7: UE connected to 5GC indicating support of UP IP over eUTRA [27](#__RefHeading___Toc42274344)

6.7.1 Introduction [27](#__RefHeading___Toc42274345)

6.7.2 Network options affected [27](#__RefHeading___Toc42274346)

6.7.3 Solution Description [27](#__RefHeading___Toc42274347)

6.7.3.1 Signalling flows [27](#__RefHeading___Toc42274348)

6.7.3.1.1 PDU Session Establishment Request procedure in 5G system [27](#__RefHeading___Toc42274349)

6.7.3.1.2 Dual Connectivity [28](#__RefHeading___Toc42274350)

6.7.4 Solution evaluation [29](#__RefHeading___Toc42274351)

6.9 Solution #9: Adding padding in the data part [30](#__RefHeading___Toc42274352)

6.9.1 Introduction [30](#__RefHeading___Toc42274353)

6.9.2 Network options affected [30](#__RefHeading___Toc42274354)

6.9.3 Solution Description [30](#__RefHeading___Toc42274355)

6.9.4 Solution Evaluation [32](#__RefHeading___Toc42274356)

6.10 Solution #10: UE activating UP IP over eUTRA to EPC [32](#__RefHeading___Toc42274357)

6.10.1 Introduction [32](#__RefHeading___Toc42274358)

6.10.2 Network options affected [32](#__RefHeading___Toc42274359)

6.10.3 Solution Description [32](#__RefHeading___Toc42274360)

6.10.4 Solution Evaluation [32](#__RefHeading___Toc42274361)

6.11 Solution #11: Support of UP IP in EPS [33](#__RefHeading___Toc42274362)

6.11.1 Introduction [33](#__RefHeading___Toc42274363)

6.11.2 Network options affected [33](#__RefHeading___Toc42274364)

6.11.3 Solution Description [33](#__RefHeading___Toc42274365)

6.11.4 Solution Evaluation [33](#__RefHeading___Toc42274366)

6.12 Solution #12: Using spare bit in existing 5G UE security capability to signal the UE support of UP IP over eUTRA to 5GC [34](#__RefHeading___Toc42274367)

6.12.1 Introduction [34](#__RefHeading___Toc42274368)

6.12.2 Network options affected [34](#__RefHeading___Toc42274369)

6.12.3 Solution Description [34](#__RefHeading___Toc42274370)

6.12.4 Solution Evaluation [34](#__RefHeading___Toc42274371)

6.14 Solution #x: LTE-EPC UP IP with option 3X/1X [35](#__RefHeading___Toc42274372)

6.14.1 Introduction [35](#__RefHeading___Toc42274373)

6.14.2 Network options affected [36](#__RefHeading___Toc42274374)

6.14.3 Solution description [36](#__RefHeading___Toc42274375)

6.14.4 Solution Evaluation [37](#__RefHeading___Toc42274376)

6.x Solution #x: 'Title of solution' [37](#__RefHeading___Toc42274377)

6.x.1 Introduction [37](#__RefHeading___Toc42274378)

6.x.2 Network options affected [37](#__RefHeading___Toc42274379)

6.x.3 Solution Description [38](#__RefHeading___Toc42274380)

6.x.4 Solution Evaluation [38](#__RefHeading___Toc42274381)

7 Conclusions [38](#__RefHeading___Toc42274382)

7.1 Conclusions on UE connects to 5GC via eUTRA [38](#__RefHeading___Toc42274383)

7.2 Conclusions on UE connects to EPC via eUTRA [38](#__RefHeading___Toc42274384)

8 Recommendations [38](#__RefHeading___Toc42274385)

Annex A: Change history [39](#__RefHeading___Toc42274386)

# 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

User Plane integrity protection allows the network operator and the UE detect that user plane data has been modified in transit between each other.

Recently, several potential attacks on the 3GPP AN interface and AN infrastructure have come to light that can be mitigated by the use of integrity protection on the User Plane over at least the radio interface. This protection is currently available for a 5G AN with a 5G core but not for LTE with EPC, LTE with a 5G Core, or for EN-DC. Integrity protection is currently specified for the control plane to protect signalling messages but is only currently specified for 5G user plane up to 64Kb per bearer.

Furthermore, supporting User Plane Integrity Protection (UP IP) at full data rate for 5G NR with 5G Core has been identified as an issue in Rel-15 and thus a UE capability-based negotiation was introduced in 5G system. Key issues and Potential enhancements to support UP IP up to the full data rate need to be studied while meeting the expected peak data throughput and lower latency as the NR and LTE radio capabilities evolve.

5G and LTE can be implemented independently and together in a number of ways. These are described in 3GPP TR 38.801 [2] (clause 7.2) and are summarised as:

- Option 1 - eUTRA with EPC

- Option 2 - NR standalone with 5G Core

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

- Option 4 - 5G core based Dual Connectivity (NR master - eUTRA secondary)

- Option 5 - 5G core with eUTRA

- Option 7 - 5G core based Dual Connectivity (eUTRA master - NR secondary)

# 1 Scope

The present document studies the key issues and potential solutions for integrity protecting the user plane, including potential enhancements needed to support UP IP up to the full data rate, in the following combinations as defined in 3GPP TR 38.801 [2] (clause 7.2):

- Option 1 - eUTRA with EPC

- Option 2 - NR standalone with 5G Core

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

- Option 4 - 5G Core based Dual Connectivity (NR master - eUTRA secondary)

- Option 5 - 5G Core with eUTRA

- Option 7 - 5G Core based Dual Connectivity (eUTRA master - NR secondary)

The present document does not detail key issues, solutions, evaluations, conclusions and recommendations for GERAN and UTRAN.

# 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 38.801:"Study on new radio access technology: Radio access architecture and interfaces".

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

[4] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[5] S3-181429, LTE and the upcoming 5G standard (GSMA).

[6] 3GPP TS 37.340: "NR; Multi-connectivity; Overall description; Stage-2".

[7] 3GPP TS 38.413: " NG-RAN; NG Application Protocol (NGAP)".

[8] 3GPP TS 38.331: "NR; Radio Resource Control (RRC) protocol specification".

[9] 3GPP TS 36.331: "Radio Resource Control (RRC); Protocol specification".

[10] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[11] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[12] 3GPP TS 23.501: "System architecture for the 5G System (5GS); Stage 2".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

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

## 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].

AN Access Network

AS Access Stratum

CP Control Plane

DRB IP Data Radio Bearer Integrity Protection

EN-DC eUTRA-NR Dual Connectivity

EPS Evolved Packet System

eUTRA evolved Universal Terrestrial Radio Access

IP Integrity Protection

NR New Radio (5G)

RAT Radio Access Technology

SMC Security Mode Command

UE User Equipment

UP User Plane

UP IP User Plane Integrity Protection

# 4 3GPP Network Options

LTE and NR networks can be implemented in many combinations, for the purpose of this document each key issue and solution is referenced to one or more of the options as defined in 3GPP TR 38.801 [2] (clause 7.2):

- Option 1 - eUTRA with EPC

- Option 2 - NR standalone with 5G Core

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

- Option 4 - 5G Core based Dual Connectivity (NR master - eUTRA secondary)

- Option 5 - 5G Core with eUTRA

- Option 7 - 5G Core based Dual Connectivity (eUTRA master - NR secondary)

# 5 Key Issues

## 5.1 Key Issue 1: UP integrity activation in EPS

### 5.1.1 Issue description

In the 5G system, as specified in TS 33.501 [4], UP security activation is separate from CP security activation and is based on a UP policy sent by the core network. In EPS, as specified in TS 33.401 [3], UP and CP AS security are activated simultaneously by the AS SMC.

For the introduction of UP integrity in EPS, it needs to be specified how UP integrity is activated in a secure way.

### 5.1.2 Network options affected

This key issue is applicable to the following network options:

- Option 1 - eUTRA with EPC

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

### 5.1.3 Threat description

If UP integrity activation is not secure, a man-in-the-middle could deceive the UE into sending UP traffic unprotected that is supposed to be protected.

### 5.1.4 Potential security requirements

The system shall support secure activation of UP integrity in EPS.

## 5.2 Key Issue #2: Secure negotiation of integrity protection support in EPS

### 5.2.1 Issue description

Integrity protection for the user plane is not supported in EPS according to TS 33.401 [3]. Neither it is possible to introduce it in a backward-compatible way. Therefore, to introduce such feature, it needs tobe considered that upgraded entities (network nodes or UEs) supporting the feature will coexist and interact with legacy ones for a long period of time. It is then expected that the network and the UE needs to be able to negotiate the support of such feature to be able to activate it in the first place. If this feature is not securely negotiated, a man-in-the-middle can deceive the network into not activating the feature. In other terms, the feature would be vulnerable to bidding-down attacks.

### 5.2.2 Network options affected

This key issue is applicable to the following network options:

- Option 1 - eUTRA with EPC

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

### 5.2.3 Threat description

In case the negotiation of the user plane integrity protection feature is not secure, a man-in-the-middle could deceive the network into not activating the feature.

### 5.2.4 Potential security requirements

The system shall support a secure negotiation of the user plane integrity protection feature while maintaining backward compatibility.

## 5.3 Key Issue 3: UE support of UP IP at the full uplink data rate

### 5.3.1 Issue description

NR (as well as the evolution of E-UTRA) is expected to support ever increasing UE peak data rates (e.g., in the order of 10's of gbps) while at the same time meeting ultra-low latency requirements for transmission of certain delay sensitive packets, e.g., use cases such as autonomous driving, industrial automation and virtual/augmented reality. For these use cases, it is important that the User Plane Integrity Protection (UP IP) can be applied at UE for the full data rate on the uplink.

In Rel-15, it was concluded that it was not possible to support UP IP at the UE supported full data rate in all cases, thus, UE capability based negotiation was introduced.

This key issue is to study solutions for supporting UP IP at the UE supported full data rate on the uplink.

NOTE: Potential solutions to address this key issue may impact RAN protocol stack. Therefore, the relevant RAN WGs needs to be consulted before concluding on any solution that addresses this key issue.

### 5.3.2 Network options affected

If DRB IP is applied at the PDCP layer also for E-UTRA, this key issue is applicable to the following network options:

- Option 1 - eUTRA with EPC

- Option 2 - NR standalone with 5G Core

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

- Option 4 - 5G core based Dual Connectivity (NR master - eUTRA secondary)

- Option 5 - 5G core with eUTRA

- Option 7 - 5G core based Dual Connectivity (eUTRA master - NR secondary)

### 5.3.3 Threat description

If UE is not able to support DRB IP at the full data rate on the UE uplink, then it will not be possible to integrity protect all DRBs on the uplink while also meeting the ultra-low latency expected by certain applications. This would allow an attacker to exploit the lack of integrity protection on the UE's uplink data transmission.

### 5.3.4 Potential security requirements

It shall be possible to apply DRB IP at the UE full data rate on the UE's uplink.

## 5.4 Key Issue 4: Integrity protection capability imbalance in enodeB connected to 5GC

### 5.4.1 Issue description

In TS 33.501 [4], NGEN-DC and NE-DC are defined as two possible MR-DC scenarios. In these cases, eNB and gNB are used in dual connectivity.

Rel.15 solution in MR-DC scenarios in TS 33.501[4] specify that, depending on the MR-DC scenario being used and the security policy at the time of PDU session establishment, the PDU session may either be rejected, the integrity protection in 5G Uu interface implicitly disabled, or the offload to SN is not allowed. The following cases summarize this behaviour according to TS 33.501[4]:

1. NGEN-DC scenario (CN=5GC, eNB=MN, gNB=SN)

a. If the UP security policy indicates UP integrity protection is "required", then the MN (MeNB) rejects the PDU session because the MN being an eNB does not support UP IP.

b. If the UP security policy indicates UP integrity protection is "preferred", then the MN (MeNB) always deactivates UP IP. The SN (SgNB) always deactivates the UP IP of any PDU session terminated at the SN. This is because MN being an eNB does not support UP IP and thus is not able to indicate to the SN (SgNB) regarding the use of UP IP.

c. If the UP security policy indicates UP integrity protection is "not needed", then the MN and SN always activates DRBs disabling the UP IP.

2. NE-DC scenario (CN=5GC, eNB=SN, gNB=MN)

a. If the UP security policy indicates UP integrity protection is "required", then if the MN (MgNB) activates the UP IP for the PDU session, then the MN (MgNB) does not offload any DRB of the PDU session to the SN (SeNB). This is because the MN (MgNB) supports UP IP, but the SN being an eNB does not support the UP IP.

b. If the UP security policy indicates UP integrity protection is "preferred", and if the MN (MgNB) activates any of the PDU session DRBs with UP IP, then the MN (MgNB) does not offload any DRB on this PDU session to the SN (SeNB). This is because the SN being an eNB does not support UP IP.

c. If the UP security policy indicates UP integrity protection is "preferred", and if the MN (MgNB) activates any of the PDU session DRBs without UP IP, the MN may offload DRBs of this PDU session to the SN (SeNB). In this case, the SN accepts the DRBs always disabling the UP IP. This is because the SN being an eNB does not support UP IP.

d. If the UP security policy indicates UP integrity protection is "not needed", then the MN and SN always activates DRBs disabling the UP IP

Therefore, Rel.15 MR-DC solution results in the situation where gNB and UE does not use UP integrity protection in some scenarios even if they're perfectly capable of supporting it on its own. This is due to the nature of combining the functionality with 2 different generation system where the older system (i.e. eNB) does not support UP integrity protection. In other words, gNB is being forced to "bid down" to a lower capability due to the presence of eNB.

### 5.4.2 Network options affected

This key issue is applicable to the following network options:

- Option 4 - 5G core based Dual Connectivity (NR master - eUTRA secondary)

- Option 7 - 5G core based Dual Connectivity (eUTRA master - NR secondary)

### 5.4.3 Threat description

In Rel.15 MR-DC solution, gNB is forced to not to use UP integrity protection in some scenarios due to the combined use of eNB which does not support UP integrity protection. This situation brings the gNB down to the same level of vulnerability as in LTE although 5G system by itself is capable of UP integrity protection.

### 5.4.4 Potential security requirements

TBD

## 5.5 Key Issue 5: Optionality of integrity protection in UP DRB with 5GC

### 5.5.1 Issue description

In Rel. 15, security architecture for 5G in TS 33.501 [4] specifies the use of UP IP. This is an improvement over LTE in light of the attack mentioned above ([5]). As specified in TS 23.501 [12], whether or not to use, UP IP in 5G system is controlled, on a PDN basis, by the (home) SMF based on parameters received from the UDM in the HPLMN. This HPLMN control is available even with Local BreakOut in the VPLMN. The capabilities of the VPLMN and the capability of the UE (as some UEs has a limitation in terms of the data rate it can support the UP IP in DRB limited to "64Kbps" in Rel.15 specification) then determine whether the PDN is established or not. This indicates that the **inadequate support of UP IP will continue to persist** as long as Rel.15 UEs with limited UP IP support exist, irrespective of new UE appearing to make it a "non-issue". However, with 5GS, the HPLMN remains in control of UPIP in a manner that is different to the HPLMN's influence over the VPLMN's encryption policy.

The use of UP IP is home network operator-dependent policy, thus optional for the network to enable for a PDU session. If the home network operator sets the policy to disable the UP IP for some reason (service-dependent policy, e.g. online Gaming, etc.), then the attack (ALTER attack) discussed in [5] is possible.

When encryption is used with no integrity protection, the attacker still could modify the UP packet. In the aLTEr attack mentioned in [5], an active attack called "user data redirection" is proposed. The attacker can modify the content of a packet if he knows the original plain text, even the packet is encrypted. In the case of DNS packets, the attacker can easily guess or find out the destination address of the original DNS server so the attacker can add a specific offset to redirect to a DNS server under the adversary's control. This is possible because the data is encrypted in a stream cipher mode, where the encryption algorithm is used as a keystream generator, and the ciphertext is computed by XORing the keystream with the plaintext.

As a result, UEs will continue to be vulnerable to potential attack exploiting the same vulnerability with LTE as discussed in [5] and also for the services where the home network operator sets the policy to disable the UP IP. In other words, as long as optionality of the UP IP exists in the system, the attack such as [5] continues to be relevant in 5G system as well, but only if the HPLMN chooses to allow this vulnerability.

### 5.5.2 Network options affected

This key issue is applicable to the following network options:

- Option 2 - NR standalone with 5G Core

- Option 4 - 5G core based Dual Connectivity (NR master - eUTRA secondary)

- Option 5 - 5G core with eUTRA

- Option 7 - 5G core based Dual Connectivity (eUTRA master - NR secondary)

### 5.5.3 Threat description

Inadequate support of UP IP will continue to persist as long as the optionality of the UP IP exists in the system. UEs not supporting UP IP at full data rate or no support of UP IP for a particular PDU session, will continue to be vulnerable to potential attacks exploiting the same vulnerability as described in [5]. In other words, as long as the optionality of the UP IP exists in the system, the attack such as [5] continues to be relevant in both 5GS and EPS.

### 5.5.4 Potential security requirements

The 5G system should support solution(s) to mitigate the threat mentioned in clause 5.5.3, when the integrity protection of a PDU session is not activated due to UE capability limitations or home network policy.

## 5.6 Key Issue 6: UE connected to 5GC indicating support of UP IP over eUTRA

### 5.6.1 Issue description

According to TS 33.501 [4] Rel-15, an NR UE and a gNB connected to 5GC, are mandated to support UP IP in NR PDCP. The use of UP IP between the UE and the gNB when connected to a 5GC is optional though. The enforcement whether to use UP IP or not, is determined by the 5G Core Network.

The eUTRA UE needs to be able to indicate to the 5GC whether it supports UP IP over eUTRA. Solutions to this key issue should specify how to do this.

### 5.6.2 Network options affected

This key issue is applicable to the following network options:

- Option 4 - 5G core based Dual Connectivity (NR master - eUTRA secondary)

- Option 5 - 5G core with eUTRA

- Option 7 - 5G core based Dual Connectivity (eUTRA master - NR secondary)

### 5.6.3 Threat description

If the network is not informed whether the UE connected to the 5GC supports UP IP over eUTRA , it may not be possible to use UP IP in this case, i.e. sensitive user plane traffic may not be integrity protected.

### 5.6.4 Potential security requirements

The 5G system shall support a mechanism for the UE connected to 5GC to indicate support of UP IP over eUTRA.

5.7 Key Issue 7: Ensuring UP IP is enforced at interworking

5.7.1 Issue description

At interworking from 5G to 4G, there is a security issue if the 5G network moves data bearers that require integrity protection to a base station connected to EPC that cannot support integrity protection. This issue is currently prevented from happening by the following requirement in clause 5.10.3 of TS 23.501 [12]:

- In the case of mobility with N26 to EPS, the source NG-RAN ensures that a PDU Session with UP integrity protection of the User Plane Security Enforcement information set to Required is not handed over to EPS.

In UEs mobility from 5G to 4G, it is necessary to ensure that UP IP will be applied to bearers that required UP IP in 5G when UP IP is supported at the target RAN node and such bearers are moved to EPS. Similarly it needs to be ensured that such bearers are integrity protected on the return to the 5G network.

5.7.2 Network options affected

This key issue is applicable to the following network options:

- Option 1 - eUTRA with EPC

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

5.7.3 Threat description

User plane traffic that requires integrity protection may be sent without integrity protection.

5.7.4 Potential security requirements

The interworking between EPS and 5GS shall ensure that integrity protection is applied to user bearers that require integrity protection.

## 5.8 Key Issue 8: HPLMN Control of UP IP usage in EPC5.X.1 Issue description

### 5.8.1

Addition of UPIP to EPC is an improvement over LTE in light of the attack mentioned above ([5]).

When encryption is used with no integrity protection, the attacker still could modify the UP packet. In the aLTEr attack mentioned in [5], an active attack called "user data redirection" is proposed. The attacker can modify the content of a packet if he knows the original plain text, even the packet is encrypted. In the case of DNS packets, the attacker can easily guess or find out the destination address of the original DNS server so the attacker can add a specific offset to redirect to a DNS server under the adversary's control. This is possible because the data is encrypted in a stream cipher mode, where the encryption algorithm is used as a keystream generator, and the ciphertext is computed by XORing the keystream with the plaintext.

Mechanisms (e.g. similar to those in 5GS) to allow the HPLMN to enforce the use of UPIP need to be investigated.

### 5.8.2 Network options affected

This key issue is applicable to the following network options:

- Option 1 - eUTRA with EPC

- Option 3

### 5.8.3 Threat description

If the HPLMN cannot enforce the use of UPIP, then they cannot guarantee protection for their subscribers against the threat mentioned in [5].

### 5.8.4 Potential security requirements

The EPS should support solution(s) to mitigate the threat mentioned in clause 5.8.3.

## 5.x Key Issue x: <Key Issue Title>

### 5.x.1 Issue description

Editor's Note: give a background to the key issue here

### 5.x.2 Network options affected

This key issue is applicable to the following network options:

- Option 1 - eUTRA with EPC

- Option 2 - NR standalone with 5G Core

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

- Option 4 - 5G core based Dual Connectivity (NR master - eUTRA secondary)

- Option 5 - 5G core with eUTRA

- Option 7 - 5G core based Dual Connectivity (eUTRA master - NR secondary)

Editor's note: delete the ones that are not applicable.

### 5.x.3 Threat description

Editor's Note: Describe threats here. Try to separate them out so that it is easy to see how the threats map to the requirements in the next section.

### 5.x.4 Security requirements

Editor's Note: add concise requirements here, preferably as a list. If you cannot define the requirements yet put an editor's note saying that the requirements are to be added.

# 6 Potential Solutions

## 6.1 Solution #1: Dedicated PDU for UP Signalling message IP

### 6.1.1 Introduction

This solution addresses key issue #5 (Optionality of integrity protection in UP DRB). This solution covers the integrity protection of the UP signalling messages, when the integrity protection of a PDU session is not activated due to UE capability limitations or serving network policy, using a dedicated integrity protection enabled PDU session.

There is impact to the UE and the AMF, to establish a dedicated integrity protection enabled PDU session.

### 6.1.2 Network options affected

This solution is applicable to the following network options:

- Option 2 - NR standalone with 5G Core

- Option 4 - 5G core based Dual Connectivity (NR master - eUTRA secondary)

### 6.1.3 Solution Description

The network configures a special DNN for exchange of secure user plane signalling messages. The UE initiates an PDU session establishment procedure to establish a separate PDU session exclusively for the user plane signalling messages and the network enables integrity protection for the PDU session. The user plane signalling messages means, for example DNS message exchanges over the UP, which requires integrity protection. Even though, the integrity protection of a PDU session is not activated due to UE capability limitations or serving network policy for a PDU session, protection of sensitive protocol message (for example, DNS exchanges) can be achieved using the dedicated PDU sessions which serves low data rate signalling exchanges, as shown in Figure 6.1.3-1.

The UE identifies/decides to send particular IP packet (UP signalling messages) over the established PDU session, based on at least one of the following Traffic Filtering information:

- application layer protocol (for example: DNS).

- Transport layer port numbers.

- Destination IP address and/or source IP address.



Figure 6.1.3-1: Dedicated PDU for UP Signalling message IP

### 6.1.4 Solution evaluation

This solution enables the integrity protection of the UP signalling messages, when the integrity protection of a PDU session is not activated due to UE capability limitations, using a dedicated integrity protection enabled PDU session. With the solution the key issue #5 (Optionality of integrity protection in UP DRB) is addressed.

The impact to the UE and the AMF is to have a new DNN configuration and it can be done as part of URSP procedure or other mechanisms, for the establishment of a dedicated integrity protection enabled PDU session, to protect the sensitive message exchanges (for example, DNS exchanges).

This solution is applicable for resource constraint Rel-15 and Rel-16 UEs, which can support integrity protection of sensitive application layer signalling messages (like DNS messages) only and does not support integrity protection of other non-signalling UP traffic.

NOTE: This solution assumes that all sensitive application layer signalling traffic are confined to 64kbps.

## 6.2 Solution #2: Integrity protection between SgNB and UE in NGEN-DC

### 6.2.1 Introduction

This solution addresses key issue #4.

In NGEN-DC scenario, in which the CN is 5GC, MN is eNB, and SN is gNB. When the UP security policy indicates UP integrity protection is "preferred", then the MN (MeNB) always deactivates UP IP. The SN (SgNB) always deactivates the UP IP of any PDU session terminated at the SN. This lead to the result that even though the UP policy is set to preferred, the PDU session is still not integrity protected between SgNB and the UE.

However, this issue can be solved through implementation way. This above issue happens in the split PDU session scenario, where some of the DRB(s) is terminated at the MN and some DRB(s) is terminated at the SN, the MN ensures that all DRBs which belong to the same PDU session have the same UP integrity protection and ciphering activation. If the network needs to protect the DRB terminated at the SgNB, it can choose to not split the PDU session.

### 6.2.2 Network options affected

This solution is applicable to the following network options:

- Option 7 - 5G core based Dual Connectivity (eUTRA master - NR secondary)

### 6.2.3 Solution description

According to TS37.340 and TS38.413, The 5GC provides two UL TEID addresses during PDU Session Resource Setup, to be applied as the first UL tunnel on the NG-U interface and the additional NG-U tunnel in case the MN decides to split the PDU session. In this message, the *Security Indication* IE is included in the *PDU Session Resource Setup Request Transfer* IE of the PDU SESSION RESOURCE SETUP REQUEST message, and the *Integrity Protection Indication* IE or *Confidentiality Protection Indication* IE is set to "required", then the NG-RAN node performs user plane integrity protection or ciphering, respectively, for the concerned PDU session. If the NG-RAN node cannot perform the user plane integrity protection or ciphering, it rejects the setup of the PDU session resources with an appropriate cause value.

Before MN decides to split the session or not, it already knows whether this PDU session needs integrity protection or not. If MN prioritize the security, it makes decision based on the *Security Indication* IE as following:

- If the *Security Indication* IE is set to "required", MN never decides to split the PUD session, but load all the DRB to SgNB to achieve the integrity.

- If the *Security Indication* IE is set to "preferred", and security has higher priority in this MN, then MN never decides to split the PDU session, but load all the DRB to SgNB to achieve the integrity.

- If the *Security Indication* IE is set to "preferred", and security has lower priority in this MN, then MN may still decide to split the PUD session.

- If the *Security Indication* IE is set to "not needed", MN may decide to split the PUD session.

Editor's Note: This solution needs to be aligned with TS33.501[4].

### 6.2.4 Solution Evaluation

Editor's note: To be added

## 6.3 Solution #3: Improved MR-DC bearer handling

### 6.3.1 Introduction

This solution addresses KI #4, Integrity protection capability imbalance in enodeB connected to 5GC.

This solution introduces enhancement to the bearer establishment and offload behaviour in Rel.15 in MR-DC scenarios. Scenarios where Rel.15 behaviour dictates suboptimal handling are addressed in such a way that the UP IP is activated whenever possible.

This solution affects the bearer establishment and offload decision in MN.

### 6.3.2 Network options affected

This solution is applicable to the following network options:

- Option 4 - 5G core based Dual Connectivity (NR master - eUTRA secondary)

- Option 7 - 5G core based Dual Connectivity (eUTRA master - NR secondary)

### 6.3.3 Solution Description

In Rel-15 MR-DC handling of UP IP, there are certain constraints exist. Specifically:

1. In NGEN-DC scenario and UP security policy is "required", then the MN (eNB) rejects bearer establishment.

2. In NGEN-DC scenario and UP security policy is "preferred", then the MN (eNB) establishes bearer without UP IP.

3. In NE-DC scenario and UP security policy is "preferred", then the MN (gNB) activates the bearer with or without UP IP. When UP IP is activated, then the MN does not offload bearer to the SN (eNB).

In all of the above scenarios, it is possible to introduce improvements to:

i) accept bearer establishment instead of rejecting it (case 1);

ii) select whether to activate UP IP or not (case 2, 3).

The improvement is described in Table 6.3.3-1 below. In all of these cases, these improvements alleviate the existing constraints in Rel.15 and introduces more cases where UP IP is activated in the bearer, enhancing the overall security of the user plane.

Table 6.3.3-1: Improvement of MR-DC handling over Rel.15 behaviour

|  |  |  |  |
| --- | --- | --- | --- |
| Case | Scenario description | Per Rel.15 MR-DC bearer handling | Improvement in this solution |
| 1 | NGEN-DC scenario (MN=eNB, SN=gNB) and UP IP CN security policy = "required" | The MeNB rejects bearer establishment. | The MeNB establishes bearer and immediately offloads it to SgNB. The MeNB instructs the SgNB to activate UP IP. The SgNB accepts the bearer with UP IP. |
| 2 | NGEN-DC scenario (MN=eNB, SN=gNB) and UP IP CN security policy = "preferred" | The MeNB establishes bearer without (i.e. deactivating) UP IP. Bearer can be offloaded to the SgNB. In this case, the SgNB accepts bearer offload from MeNB without UP IP. | The MeNB establishes bearer either with or without UP IP.  If the MeNB establishes bearer with UP IP, the MeNB immediately offloads it to SgNB. The MeNB instructs the SgNB to activate UP IP. The SgNB accepts the bearer with UP IP.  If the MeNB establishes bearer without UP IP, the MeNB can offload it to SgNB. The MeNB instructs the SgNB to activate UP IP. The SgNB accepts the bearer optionally with UP IP. |
| 3 | NE-DC scenario (MN=gNB, SN=eNB) and CN UP IP security policy = "preferred" | If the MgNB activates bearer with UP IP, the MgNB does not offload bearer to the SeNB.  If the MgNB activates without (i.e. deactivating) UP IP, the MgNB can offload bearer to the SeNB. The SeNB accepts the bearer offload without UP IP. | If the MgNB activates bearer with UP IP, the MgNB may offload the bearer to the SeNB. The SeNB accepts the bearer without UP IP.  If the MgNB activates without (i.e. deactivating) UP IP, the MgNB can offload bearer to the SeNB. The SeNB accepts the bearer offload without UP IP. |

Editor's Note: clarification on termination point of offloaded bearers needs to be added.

Editor's Note: additional detail on bearer establishment and offload needs to be described.

Editor's Note: additional clarification to notes on #3 needs to be added.

### 6.3.4 Solution evaluation

Editor's Note: TBD.

## 6.4 Solution #4: Zero-overhead user plane integrity protection on the link layer

### 6.4.1 Introduction

Existing attacks on UP-IP require a man-in-the-middle (MitM) relay that is located between UE and eNB. The MitM relay receives packets from the UE/eNB, modifies them, and forwards them towards eNB/UE. Thus, techniques that defeat MitM relay attacks defeat also attacks on UP-IP. The "Zero-overhead user plane integrity protection on the link layer" solution does this -- it defeats MitM relay attacks -- by replacing the CRC associated to each transport block in L2 by a cryptographic CRC denoted CRC' and linked to the transport block ***identity*** itself. By doing this, an attacker cannot receive a packet, process and modify it, and forward it in a later transport block since this changes the transport block *identity* used, and thus, the verification of the cryptographic CRC fails.

This solution addresses the key issue #3: "UE support of UP IP at the full uplink data rate" and key issue #5: "Optionality of integrity protection in UP DRB".

Key issue #3 is addressed since it provides protection against attacks on UP IP even at full uplink data rate. Key issue #5 is addressed since this protection is applied to all UP DRBs.

The proposal is to use a cryptographic CRC instead of the regular CRC in Transport Blocks on the user plane.

This solution reduces the overhead of integrity protection to ZERO.

The effective user data throughput remains the same as without the integrity protection.

The error behaviour of the Link layer remains exactly the same as without the proposed integrity protection.

This solution requires the addition of the computation of a MAC over or the encryption of 128 bits per CRC in a Transport Block so per 6144 bits, which is a reduction of about a factor 50 in the amount of computations required for the UP IP of a PDCP packet. It can therefore be used at full uplink data rates and is a solution to key issue 3.

With this solution, all Transport Blocks independent of the data rate can be integrity protected, so automatically, all PDCP packets become integrity protected and the integrity protection does not have to be a serving network operator-dependent policy anymore, which solves the UP IP optionality KI#5.

**Some background**

- A Transport Block is defined as the basic data unit exchanged between L1 and MAC. An equivalent term for Transport Block is "MAC PDU".

- Each Transport Block has a CRC over the total TB. Most TBs, including User Data TBs, have a 24-bit CRC.

- Transport Blocks are subdivided in Code Blocks if larger than 6144 bit. Each CB has its own 24-bit CRC.

- A Resource Block pair is the unit for the scheduling of resources by the base station.

- One Resource Block consists of 12 successive OFDM sub-carriers in frequency and one slot of 0.5 millisecond in time

72 or 84 OFDM symbols per RB of 1 to 10-bit each.

- A Resource Block pair consists of the two successive RBs in the two successive slots of a subframe of 1 millisecond.

- If a Transport Block is larger than a Resource Block pair, more RB pairs are added in the frequency direction.

 Each TB is limited to a subframe of 1 millisecond.

- TBs with an incorrect CRC are discarded by the receiver and a retransmission is requested (Hybrid Automatic Repeat-Request (HARQ)).

- An LTE frame consists of 10 subframes.

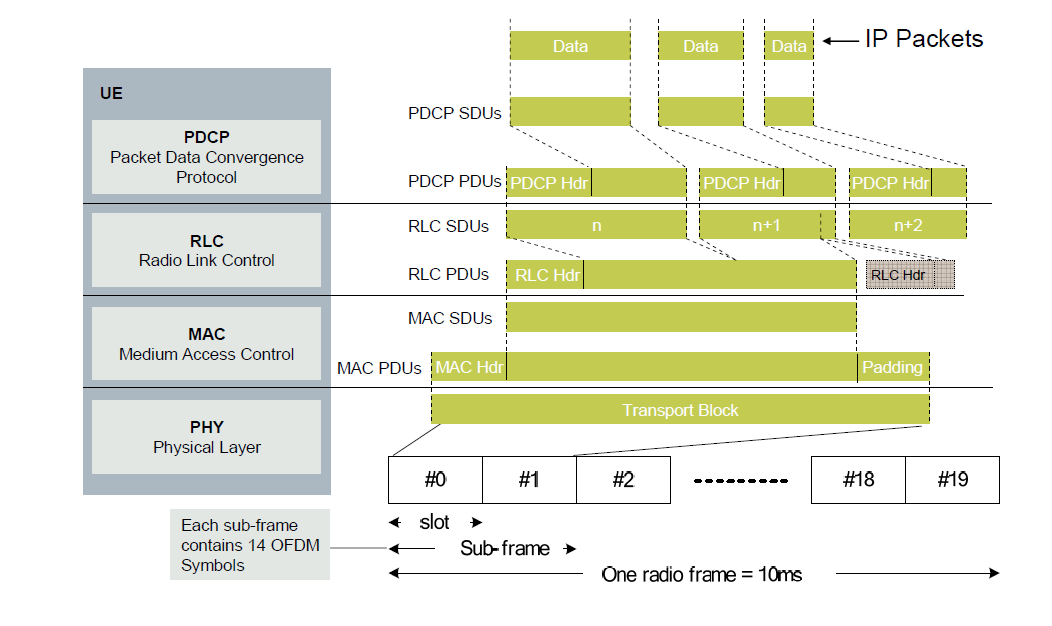


Figure 6.4.1-2: LTE packet structure relating PDCP packets to Transport Blocks

### 6.4.2 Network options affected

This solution is applicable to the following network options:

- Option 2 - NR standalone with 5G Core

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

- Option 4 - 5G core based Dual Connectivity (NR master - eUTRA secondary)

- Option 7 - 5G core based Dual Connectivity (eUTRA master - NR secondary)

### 6.4.3 Solution description

It is proposed to use a cryptographic version of the CRC in every user Transport Block.

This can be achieved by replacing the 24-bit CRCs in a Transport block by 24-bit CRC's as computed by

CRC' = truncate { 24, HMAC( K, CRC | TransportBlockID) } (1)

or

CRC' = truncate { 24, Encrypt( K, CRC | TransportBlockID) } (2)

In addition, the CRCs of the Code Blocks inside a TB may also be replaced by their cryptographic versions.

Encryption requires probably less effort than HMAC. The encryption is done in ECB mode. A truncated encryption is OK, the truncated encryption serves as a CRC. Both sender and transmitter compute the CRC' using truncated encryption of equation (2). The transmitter puts the computed CRC' at the CRC field of the TB. The receiver computes it too according to equation (2) and compares this with the CRC' value in the CRC field of the received TB. If they are the same, the integrity protection check passes, else it fails. Therefore, because there is no decryption required, only checking whether truncated encryptions are the same or not.

Mobility problem (different key per gNB)

The key K to use is derived from a master key such that the derivation is dependent on the gNB or the DU inside the gNB. The master key is different for each UE (or UICC/USIM), but is used only for the UPIP functionality in this solution. gNBs or DUs get provisioned with the key K derived for them. The UE (or UICC/USIM) is provisioned with the master key and does the derivation of the key K itself.

Rekeying of the master key

The master key needs to be rekeyed before the time dependent part of TransportBlockID rolls over. An HSFN + 11 extra bits leads to a roll-over every 1.4 year.

Bundling of PDCP-PDUs

The master key and the key K are not dependent on the content of a TB, i.e. the PDCP-PDUs that are carried inside that TB.

Dual connectivity (split bearer) situation

In case of dual connectivity (split bearer), TBs that are sent over a bearer that does support this solution are integrity protected, while TBs that are sent over a bearer that does not support this solution are not protected.

The TransportBlockID is used to prevent an attacker to collect entries for a CRC -> CRC' dictionary.

Requirements for the TransportBlockID are the following two.

1. TransportBlockID should be different for different slots or subframes.

2. TransportBlockID should be different for TBs of the same user in the same slot or subframe.

Candidates for requirement 1 that are simple to retrieve by both UE and eNodeB may be:

- the subframe number (0 - 9) that the TB starts in;

- the System Frame Number (SFN) (0 - 1023) that the TB starts in (repeats every 10.24 seconds);

- the hyper-SFN (HSFN) (0 - 1023) that the TB starts in (repeats about every 3hours; the HSF is also used as part of the COUNT in the PDCP integrity protection);

- a new sequence number similar to the hyper-SFN (HSFN) and made available in a system message to all devices in a cell similar to the way the HSFN or the SFN is made known (HSFN + 11 extra bits leads to a roll-over every 1.4 year);

- a new sequence number made available through an AS secured RRC message;

- a Radio Network Temporary Identifier (RNTI), either existing or new one, only known to the UE and the gNB, that gets updated frequently;

- the length of the TB;

- the slot number (0 or 1) of the slot the TB starts in (?);

- etc.

Candidates for requirement 2 that are simple to retrieve by both UE and eNodeB may be:

- indication of uplink or downlink bit;

- indication whether the CRC/CRC' is for the entire TB or for a Code Block (sub part of TB with its own CRC);

- CB number in case the CRC/CRC' is for a CB;

- indication whether the TB is the first (0) or second (1) TB to/from a device in this subframe;

- lowest (or highest) frequency of all sub carriers used for the entire TB;

- number of subcarriers and/or Resource Blocks used for the entire TB;

- number of the spatial stream or the antenna port number in case of spatial multiplexing;

- carrier indicator indicating the carrier this TB is transferred on in case of carrier aggregation;

- PLMN ID, or Cell Identity;

- Evolved Cell Global Identifier = PLMN ID concatenated with the Cell Identity;

- physical layer cell identity (0 - 503);

- base station name (eNodeB name) as transmitted in the System Information Block 9 (SIB9);

- etc.

Control of the Transport Block level integrity protection provided by this solution.

When the system wants to use the UP-IP at the Transport Block level of this solution between a certain UE and gNB, it starts a PDCP entity just for this purpose, while using one integrity algorithm identifier of a set of new integrity algorithm identifiers in the integrityProtAlgorithm attribute in the SecurityAlgorithmConfig information element (clause 6.3.3 of TS 36.331 [9]), see "Negotiation of UP-IP" below. Any of the existing ciphering algorithm identifiers can be used for the cipheringAlgorithm attribute.

This PDCP entity, as any other PDCP entity, may be used for the transfer of IP packets. All of these packets are integrity protected at the Transport Block level.

When the system wants to use different bearers, with different policies and QoS, etc., it can do so as it was used to. But when the system starts a PDCP entity with one of the new nia4, nia5, nia6, nia7 integrity algorithm identifiers, all Transport Blocks to and from the UE are going to use the cryptographic CRC. This does not influence the data rates/QoS of the other PDCP entities. In case another PDCP entity did not use PDCP UP-IP protection, it has now UP-IP based on the cryptographic CRC. In case it already had PDCP UP-IP, it now also has UP-IP based on the cryptographic CRC at the TB level.

If performing cryptographic CRC is not desired for all user plane data (even though this is identified as possibly problematic in KI#5), then the security policy per PDU session may be extended to include a flag which indicates whether to apply cryptographic CRC or not. A UE that supports multiple MAC entities (as described in TS 38.321), which the UE may already have in order to support e.g. multi-RAT connections or dual connectivity, can use one MAC entity to serve all PDU sessions with integrity protection switched on, and another MAC entity to serve all PDU sessions with integrity protection switched off. If a UE that does not support multiple MAC entities wants to establish an additional PDU session, and the additional PDU session has a different value for cryptographic CRC in the security policy as the already established PDU session(s), then the UE may choose to wait or cancel the additional PDU session until the existing PDU session is torn down and the MAC entity becomes available, and may inform the user that the additional PDU session cannot be established due to device limitations. Alternatively, the AMF can be made aware of such device limitation and update the security policy such that the UE will change to using PDCP based integrity protection instead of using cryptographic CRC, possibly at a lower data rate, due to overhead that this may bring.

Negotiation of UP-IP

The application of this solution can be negotiated and controlled with the same procedures as those for the PDCP integrity protection with the following extensions for NR. Similar extensions may be made for E-UTRA.

- The F1-C interface is extended with one or more new messages to supply the DU with the required information for the integrity protection of this solution.

- The list of integrity algorithm identifiers in clause 5.11.1.2 of [4] is extended with one or more of the following values:

- "01002" 128-NIA4 128-bit SNOW 3G based algorithm using equation (2) above in ECB mode;

- "01012" 128-NIA5 128-bit AES based algorithm using equation (2) above in ECB mode;

- "01102" 128-NIA6 128-bit ZUC based algorithm using equation (2) above in ECB mode; and/or

- "01112" 256-NIA7 HMAC-SHA256 based algorithm using equation (1) above.

- The list of integrity algorithm identifiers in the integrityProtAlgorithm attribute in the SecurityAlgorithmConfig information element (clause 6.3.3 of TS 36.331 [9]) is extended with the same new value(s) as the ones in the previous bullet.

- The *integrityProtAlgorithm* enumeration in the IE *SecurityAlgorithmConfig* in clause 6.3.2 of [8] is extended with nia4, nia5, nia6, and/or nia7, consistent with the extension of the list of integrity algorithm identifiers as described the bullet above.

Consequence of UP-IP termination in the DU

Since the negotiation of the application of this solution is done in the PDCP layer, but the application itself in the DU, the F1-C interface is extended with one or more new messages to supply the DU with the required information for the integrity protection of this solution.

This solution provides integrity protection between the UE and the DU. The integrity protection can be extended to the CU, by applying IPsec on the F1-U interface, as specified in clause 9.8.2 of [4].

Since the key K is part of the information to be sent on the F1-C interface to the DU, the security mechanisms as specified in clause 9.8.2 of [4] for the F1-C interface need to be applied as well.

The contents of a TB with an incorrect cryptographic CRC is blocked by the DU from further transmission to the CU.

Key hierarchy and key management

The key K in equation (1) or (2) above can be taken as the key KUPint as specified in [4].

However, this would mean that PDCP UP-IP and the integrity protection of this solution cannot be used at the same time. Therefore, a new key KTBint may be defined in [4] that is managed and derived in the same way as KUPint except that a value of 0x07 is used for the algorithm type distinguisher in clause A.8 of [4] instead of 0x06.

### 6.4.4 Solution Evaluation

The impact on the protocol stack (PHY + MAC + RRC)

The PHY in the UE and in the DU needs to be extended with means to generate the CRC' in outgoing Transport Blocks and means to check the CRC' of incoming Transport Blocks according to equations (1) and/or (2) above. This means that for every CRC computed, an additional HMAC needs tobe computed if equation (1) is used or one encrypted value needs to be computed if equation (2) is used.

Since the cryptographic CRC computation is based on the (linear) CRC itself, XOR-ing a TB that is protected with the cryptographic CRC with a TB with a zero-valued CRC will lead to a TB that passes the integrity check.

The PHY in the UE needs to be extended with means to receive the information required to apply and cease to apply the integrity protection of this solution from the RRC layer in the UE.

The PHY in the DU and the RRC in the CU need to be extended with means to exchange the information required to apply and cease to apply the integrity protection of this solution using one or more new messages over the F1-C interface. Since the key K is part of this information, the security mechanisms as specified in clause 9.8.2 of [4] for the F1-C interface need to be applied.

The RRC in the UE and CU need to be extended with the new integrity algorithm identifier(s) specified for this solution.

There is no change required in the MAC, but it may be desirable for a UE to support multiple MAC entities..

The integrity protection strength of this solution is less than that of the PDCP MAC, namely 24 bit instead of 32 bit.

The security properties of using the cryptographic CRC as an integrity protection have not been evaluated.

This solution addresses the key issue #3: "UE support of UP IP at the full uplink data rate" and key issue #5: "Optionality of integrity protection in UP DRB".

The proposal is to use a cryptographic CRC instead of the regular CRC in Transport Blocks on the user plane.

This solution reduces the overhead of integrity protection to ZERO.

The effective user data throughput remains the same as without the integrity protection.

The error behaviour of the Link layer remains exactly the same as without the proposed integrity protection.

This solution requires the addition of the computation of a MAC over or the encryption of 128 bits per CRC in a Transport Block so per 6.144 bits, which is a reduction of about a factor 50 in the amount of computations required for the UP IP of a PDCP packet. It can therefore be used at full uplink data rates and is a solution to key issue 3.

With this solution, all Transport Blocks independent of the data rate can be integrity protected, so automatically, all PDCP packets become integrity protected and the integrity protection does not have to be a serving network operator-dependent policy anymore, which solves the UP IP optionality KI#5.

## 6.5 Solution #5: Integrity Protection of packet header in the User Plane

### 6.5.1 Introduction

This solution addresses key issue #5 (Optionality of integrity protection in UP DRB). The solution only protects the integrity of the packet header when data rate is over 64 kbit/s.

### 6.5.2 Network options affected

This solution is applicable to the following network options:

- Option 2 - NR standalone with 5G Core

### 6.5.3 Solution Description

The protocol stack of the user plane in 5G network differs from the protocol stack of the user plane in 4G network in that a Service Data Adaptation Protocol (SDAP) is added as shown in the Figure 6.5.3-1. The role of SDAP [2] is to map the QoS flow to the Data Radio Bearer (DRB) and mark the QoS flow identifier (ID) in the SDAP header. It provides a finer-grained management of QoS than 4G with respect to the user plane data.



Figure 6.5.3-1: Protocol stack

After the user plane packet is encapsulated, the PDCP layer packet format is as follows:



Figure 6.5.3-2: Packet format in the PDCP layer

Where HPDCP is the header of PDCP layer, HSDAP is the header of the SDAP layer, and Hdata is the header of the packet. The PDCP sequence number (PDCP SN) in the HPDCP is part of the packet count value COUNT. To protect the header of the packet, the following parameters are input to the integrity function (e.g. NIA1) to produce MAC-I.

- COUNT，

- MESSAGE

- DIRECTION

- BEARER

- KEY

Where MESSAGE is to be integrity protected, which is the cascade of the HSDAP and Hdata.

### 6.5.4 Solution Evaluation

The proposed scheme can be evaluated in context of security, efficiency, and compatibility as follows:

**- Security**

The proposed scheme addresses key issue #5 (Optionality of integrity protection in UP DRB) by integrity protecting the header part of the PDCP data. Besides the packet header of UP IP signalling messages (DNS query packets), the subsequent IP header of the data are integrity protected. Moreover, the packet headers for some applications that does not have DNS query procedure are also integrity protected. As a result, the attacks that wants to route the packets to a wrong destination by modifying the packet header can be prevented. However, this solution does not protect the whole packet, thus the modification on the payload part could not be mitigated.

**- Efficiency**

- This solution provides a means to integrity protect IP header part of the PDCP data payload. The proposed scheme is more efficiency than the scheme specified in TS 33.501. This is because only the packet header is integrity protected, while the whole packet is integrity protected in TS 33.501. However, the PDCP layer needs to look inside the PDCP payload to determine the payload type (e.g., non-IP, IPv4 or IPv6) and this adds additional overhead.

**- Compatibility**

- This solution faces difficulty to implement as PDCP layer could not identify the type of upper layer data. It could neither recognize whether the data is IP packet or non-IP packet, nor whether IP packet is IPv4 packet or IPv6 packet. That means it is hard to define which part of PDCP head should be integrity protected.

Editor's note: Further evaluation is FFS

## 6.6 Solution #6: Addition of UP IP for eUTRA with 5GC

### 6.6.1 Introduction

To protect user plane communication reliably in Options 4, 5 and 7 and to maintain compatibility with NR, this solution describes the addition of User Plane integrity protection to eUTRA in a similar way to the 5G implementation.

### 6.6.2 Network options affected

This solution is applicable to the following network options:

- Option 4 - 5G core based Dual Connectivity (NR master - eUTRA secondary)

- Option 5 - 5G core with eUTRA

- Option 7 - 5G core based Dual Connectivity (eUTRA master - NR secondary)

### 6.6.3 Solution Description

The clauses regarding user plane integrity protection for eUTRA are added as detailed for NR in 3GPP TS 33.501[4].

Editor's Note: More details regarding this solution are to be added

### 6.6.4 Solution Evaluation

Editor's Note: to be added

## 6.7 Solution #7: UE connected to 5GC indicating support of UP IP over eUTRA

### 6.7.1 Introduction

This solution addresses key issue #6 (UE connected to 5GC indicating support of UP IP over eUTRA). This solution describes how the UE provides its capability to the network to indicate that it supports UP IP over eUTRA when connected to 5GC.

According to TS 33.501 [4], UP IP is mandatory to be supported for the gNB and the UE., The UE indicates its capability for maximum data bitrate for UP IP over NR to the 5G network in NAS layer. Its FFS whether this capability applies to eUTRA supporting UP IP as well or whether a new capability is required for eUTRA.

As UP IP in a ng-eNB connected to 5GC is currently not specified in TS 33.501 [4], this implies that even if a Rel-15 UE would have supported UP IP over eUTRA, there was no possibility for a Rel-15 UE to test UP IP over eUTRA in any live 5G Rel-15 network, therefore its envisioned that a Rel-15 UE has not enabled UP IP over eUTRA (connected to a 5GC). A capability indication is required for a Rel-16 UE which supports UP IP over eUTRA (connected to a 5GC) in order for a Rel-16 network to be able to distinguish between a Rel-15 UE which cannot enable UP IP over eUTRA and a Rel-16 UE which can enable UP IP over eUTRA.

This solution assumes that the UE has been upgraded to support UP IP over eUTRA connected to 5GC. It also assumes that the ng-eNB supports UP IP and supports the capability of enabling UP IP with the UE over eUTRA.

There is impact on UE, SMF, AMF and ng-eNB/gNB.

### 6.7.2 Network options affected

This solution is applicable to the following network options:

- Option 4 - 5G core based Dual Connectivity (NR master - eUTRA secondary)

- Option 5 - 5G core with eUTRA

- Option 7 - 5G core based Dual Connectivity (eUTRA master - NR secondary)

### 6.7.3 Solution Description

#### 6.7.3.1 Signalling flows

##### 6.7.3.1.1 PDU Session Establishment Request procedure in 5G system

The UE initiates the PDU Session establishment procedure with the SMF, via the AMF, to establish data bearers with the network. If the UE supports UP IP over eUTRA when connected to a 5GC, then the UE includes its capability to support UP IP over eUTRA in the PDU Session Establishment Request message to the SMF.



Figure 6.7.3.1.1: UE indicating support of UP IP over eUTRA when connected to 5GC

1. UE initiates PDU Session Establishment procedure with the SMF to establish bearers with the network and includes its capability to support UP IP over eUTRA when connected to 5GC into PDU Session Establishment Request message.
2. The SMF initiates the N2 PDU Session Request procedure with ng-eNB/gNB and includes the UE capability to support UP IP over ng-eNB when connected to 5GC. The SMF also includes the UP security policy.
3. The ng-eNB/gNB initiates RRC Reconfiguration procedure with the UE and indicates to the UE to activate UP integrity protection for the DRBs (data radio bearers) established with the ng-eNB/gNB.

#### 6.7.3.1.2 Dual Connectivity

If a ng-eNB acting as a MN receives the UE capability from the 5GC indicating that the UE supports UP integrity protection over eUTRA, then the MN takes that capability into consideration together with the UP security policy, when it makes the decision whether to activate UP integrity protection for its own DRB's established with the UE.

For the scenario when 'no split PDU session' takes place, the handling of the UP security policy should be the same as for as described in clause 6.10.2.1 in TS 33.501 [4].

In the scenario of 'no split PDU session' when MN offloads DRB(s) for a PDU session to a ng-eNB acting as a SN, there are two options to consider as described below.

ALTERNATIVE 1:

The MN determines from the UP security policy and the UE capability indicating that the UE supports UP integrity protection over eUTRA, both received from the 5G Core Network, and also the capability of the SN i.e. whether it supports UP IP or not, before the MN decides to offload any DRB(s) of the PDU Session to the SN which requires UP integrity protection.

ALTERNATIVE 2:

The MN forwards the UE capability indicating that the UE supports UP integrity protection over eUTRA and the UP security policy, both received from the 5G Core Network, to the ng-eNB acting as a SN. The SN will make the decision of activating UP integrity protection or not for the PDU sessions that are terminated at the SN.

In the scenario of 'split PDU session' when MN offloads some of the DRB(s) for a PDU session to a ng-eNB acting as a SN, the handling of the UP security policy should be the same as for NR-DC as described in clause 6.10.4 in TS 33.501 [4].

### 6.7.4 Solution evaluation

The solution fulfils the requirement in key issue #6 (UE connected to 5GC indicating support of UP IP over eUTRA).

The impact of the solution is to require the UE to indicate its support of UP IP over eUTRA when connected to 5GC, to the ng-eNB/gNB via NAS layer. There is impact on UE, SMF, AMF and ng-eNB/gNB.

According to TS 33.501 [4], the UE indicates its capability for maximum data bitrate for UP IP over NR to the 5G network in NAS layer. Its FFS whether this capability applies to eUTRA supporting UP IP as well or whether a new capability is required for eUTRA. This is for other groups as CT1 and RAN2 to decide.

As UP IP in a ng-eNB connected to 5GC was not enabled in Rel-15, this implies that even if a Rel-15 UE would have supported UP IP over eUTRA, there was no possibility for a Rel-15 UE to test UP IP over eUTRA in any live 5G Rel-15 network, therefore its envisioned that a Rel-15 UE has not enabled UP IP over eUTRA connected to a 5GC. A capability indication is required for a Rel-16 UE which supports UP IP over eUTRA connected to a 5GC, in order for a Rel-16 eUTRA to be able to distinguish between a Rel-15 UE which cannot enable UP IP over eUTRA and a Rel-16 UE which can enable UP IP over eUTRA. This is for other groups as CT1 to decide.

For the scenario when 'no split PDU session' takes place, the handling of the UP security policy should be the same as described in clause 6.10.2.1 in TS 33.501 [4]. The MN always forwards the UE capability including the UP security capability and the UP security policy to the SN. The SN makes the decision whether to activate UP integrity protection or not, and also whether to activate UP encryption or not. Therefore, it is proposed to go forward with alternative 2 in clause 6.7.3.1.2.

In the scenario of 'split PDU session' when MN offloads some of the DRB(s) for a PDU session to a ng-eNB acting as a SN, the handling of the UP security policy should be the same as for NR-DC as described in clause 6.10.4 in TS 33.501 [4].

The ng-eNB and the 5G core network could be of different releases, e.g.:

- a Rel-15 ng-eNB connected to a Rel-16 5G core network;

A Rel-15 ng-eNB cannot activate UP integrity protection with a Rel-16 UE supporting UP IP over e-UTRA for any established DRB's with the Rel-16 UE. A Rel-15 ng-eNB would ignore any additional capability or indication from a Rel-16 5G core network which indicates the Rel-16 UE supports UP IP over e-UTRA.

- a Rel-16 ng-eNB connected to a Rel-15 5G core network;

A Rel-16 ng-eNB cannot activate UP integrity protection with a Rel-16 UE supporting UP IP over e-UTRA for any established DRB's if the Rel-16 ng-eNB is connected to a Rel-15 5G core network. A Rel-15 5G core network would ignore any additional capability or indication from a Rel-16 UE which indicates the Rel-16 UE supports UP IP over e-UTRA and would not be able to indicate to the Rel-16 ng-eNB that the Rel-16 UE supports UP IP over e-UTRA).

This solution requires that both 5G core network and ng-eNB are upgraded in order to be able to activate UP IP over E-UTRA.

6.8 Solution #8: Using existing 5G UE security capability to signal the UE support of UP IP over eUTRA to 5GC

6.8.1 Introduction

This solution addresses key issue #6 (UE connected to 5GC indicating support of UP IP over eUTRA).

This solution only impacts the UE and the ng-eNB.

6.8.2 Network options affected

This solution is applicable to the following network options:

- Option 4 - 5G core based Dual Connectivity (NR master - eUTRA secondary)

- Option 5 - 5G core with eUTRA

- Option 7 - 5G core based Dual Connectivity (eUTRA master - NR secondary)

6.8.3 Solution description

The solution is to use one of the bits that is used to indicate support of an EEA or EIA algorithm that is currently not used in 5G UE Security Capability IE (see 9.11.3.54 of TS 24.501 [10]) to indicate that the UE supports user plane integrity protection with an ng-eNB.

This information element is already protected to the core network in NAS signalling and also replayed to the UE to ensure Man-in-the-middle attacks are avoided. It is also already signalled to the RAN nodes so would require no additional signalling.

6.8.4 Solution evaluation

This solution meets the security requirement for key issue #6 and only impacts the UE and the ng-NB as it reuses the existing NAS signalling and the information element in a secure manner to indicate UE's support of user plane integrity protection over eUTRA to the network.

## 6.9 Solution #9: Adding padding in the data part

### 6.9.1 Introduction

This solution addresses key issue #5.

The aLTEr attack mentioned in [5], an active attack called "user data redirection" is proposed, in which the attacker could change the DNS packet address even when the packet is encrypted.

The proposed issue is caused by adequate of integrity protection. When there is no UP IP, the attacker could change the destination address even the encryption is used. The solution is proposing to add some random length padding, thus the attacker would not know which part is the destination address when the validation time is limited to a tight higher bound.

### 6.9.2 Network options affected

This solution is applicable to the following network options:

- Option 2 - NR standalone with 5G Core

- Option 4 - 5G core based Dual Connectivity (NR master - eUTRA secondary)

- Option 7 - 5G core based Dual Connectivity (eUTRA master - NR secondary)

### 6.9.3 Solution Description

5G NR PDCP PDUs is formatted as mentioned in 3GPP TS 38.323 clause 6.2.2. Hence, each PDCP data PDU will be composed of PDCP SN, data payload and an optional 4B MAC-i payload. As per spec, data unit that is ciphered is the data part of the PDCP Data PDU except the SDAP header if included in the PDCP SDU, and the MAC-I.

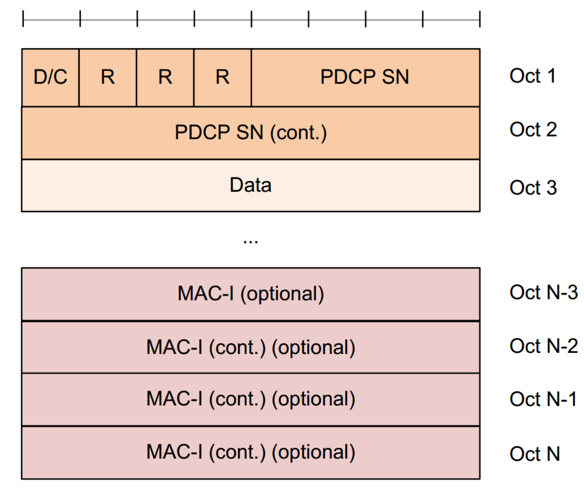


Figure 6.9.3-1: PDCP data PDU format (refer to TS38.331)

In a new implementation, it is possible to add padding bytes to data part(The data part includes the IP header and will be encrypted). These padding bytes and the Padding Size LI can be part of the cipher payload. One example of such an implementation is as follows:

- One of the "R" bits in the PDCP header can be used to indicate if Padding is included.

- One of the "R"bits in the PDCP header can be used to indicate the whole length of the PDU.

- Padding Size is added at the octet "N-4". It can range from 0 - 255 octets. The first half is used to indicate how many bits is added before the data part, and the second half is used to indicate how many bits is added after the data part.

- Non-Zero Initialized Padding Bytes (based on Padding Size) are added after the data part of the PDCP PDU.

- Transmit PDCP entity can determine "randomly" a value from 0 - 255 bytes of padding.

In some implementations, padding size could be limited to a maximum of "x" % of the original PDCP PDU to avoid wasting bandwidth. Padding could be configured by the network in RRC Signaling.

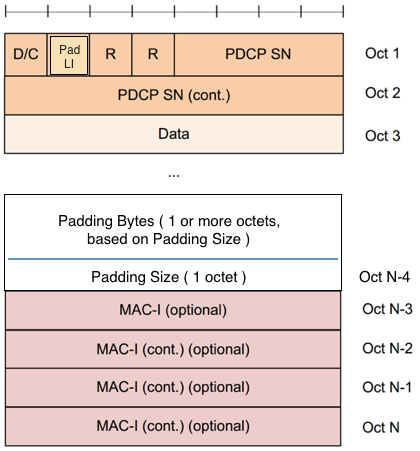


Figure 6.9.3-2: New PDCP data PDU format

With this mechanism, the attacker could not know where to put the offset since all the data part is encrypted and the destination address is not in the first few bits anymore. However, the attack could still try [the length of the padding] times to verify where exactly the true data part. So the solution could be enhanced with adding the limitation of validation times. Thus even if the attacker does not corrupt the padding, they'll just end up corrupting the SDU itself unless they guess exactly the right offset.

### 6.9.4 Solution Evaluation

PDCP PDU maximum size is 9000byte, when the IP packet is less than 8744byte, there will be no impact.

Editor's Note: This solution doesn't work when confidentiality is not used.

Editor's Note: Further evaluation is FFS.

## 6.10 Solution #10: UE activating UP IP over eUTRA to EPC

### 6.10.1 Introduction

This solution addresses KI#2 (Secure negotiation of integrity protection support in EPS).This solution describes how the UE tells the eUTRA the support of UP IP, and how the eUTRA activates the UP IP with the UE.

### 6.10.2 Network options affected

- Option 1 - eUTRA with EPC

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

### 6.10.3 Solution Description

In TS 33.401 [3], UP encryption is activated after UE successfully verifies the integrity protection of the AS SMC message. This means that UP ciphering is always on for UE connects to EPC via eUTRA. But for activating UP IP in eUTRA when UE connects to EPC, the "always on" feature for UP integrity will consume a lot of resources and reduce the user experience. Therefore, the similar scheme as defined in TS 33.501 [4] is introduced, which is the eUTRA will control whether the UP IP is activated or not. But due to the impact on EPC should be limited, which means the MME should not be mandatory to be upgraded to send the UP security policy to the eUTRA, so the eUTRA is based on its configuration to decide whether the UP IP is activated or not.

The eUTRA recognizes whether the UE supporting UP IP by reading the UE capability IE. As there are 4 reserved bits in UE capability IE, one of them can be used by the UE to indicate whether the UP IP is supported by this UE.

If the eUTRA finds the UE supporting UP IP feature and decides the UP IP is activated, then it will signal the UE in AS SMC.

Editor's Note: It is FFS that how the eUTRA make decisions on the UP IP policy.

The UE will activate the UP IP after successfully checks the integrity of AS SMC, and the eUTRA will activate the UP IP after sending the AS SMC.

### 6.10.4 Solution Evaluation

TBD

## 6.11 Solution #11: Support of UP IP in EPS

### 6.11.1 Introduction

This solution addresses key issue #1 (UP integrity activation in EPS). A UE which has been upgraded to support UP IP over LTE access, when connected to EPS, needs to indicate UE support of UP IP to the network.

This solution impacts the UE, the MME, the HSS and the LTE eNB.

### 6.11.2 Network options affected

This solution is applicable to the following network options:

- Option 1 - eUTRA with EPC

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

### 6.11.3 Solution Description

The UE capability to support UP IP over LTE access when connected to EPS could be indicated in Attach Request and Tracking Area Update Request message. A new IE could be included in the Attach Request message and Tracking Area Update Request message. The new IE would need to be mapped on the S1 interface to the LTE eNB.

The transfer of the new IE would also have impact on S10 interface between MME's. For coexistence with legacy nodes then support needs to be signalled by the UE again during mobility procedures at MME change, but this should not be a problem as the UE would initiate a new Tracking Area Update procedure at MME change anyway. Also, it is not envisioned that the LTE eNB would be upgraded, without upgrading the MME as well.

The MME could apply/request use of UP IP at PDN Connection establishment (on par with 5GS). UP IP would then be applied per PDN connection lifetime.

The MME could configure a security policy for UP IP i.e. a UP IP policy, per APN and/or the MME could determine the UP IP policy by potentially retrieving a UP IP policy for the subscription stored in the HSS or from the locally configured UP IP policy. The determined UP IP policy would be configured per UE. The UP IP policy could use similar setting options as in 5GS: "required", "preferred", "not needed".

The MME provides the determined UP IP policy per UE to the LTE eNB on the S1 interface.

The UP IP policy could be extended to a UP security policy which includes a security policy for UP encryption as well. This would harmonize the feature over both systems (EPS and 5GS).

The enabling/disabling of UP IP for DRB's is done using AS SMC procedure and RRC Reconfiguration procedure, similar as in NR.

### 6.11.4 Handling of legacy UE’s and legacy network nodes in EPS

It is expected that if the eNB is upgraded to support UP IP, then the connected MME is upgraded as well to support the UP security policy (i.e. UP IP). A legacy eNB which is not supporting UP IP, is most likely connected to MME which is not supporting the UP security policy (i.e. UP IP).

**Legacy UE’s:**

A legacy UE which establishes a new PDN connection with an upgraded MME and eNB (to support UP IP), should be handled by the MME and the eNB in the legacy way, and this decision could be based upon a configured operator policy. If the configured operator policy allows the upgraded MME/eNB to handle the legacy UE, then the MME cannot determine a UP IP policy to "required" as UP IP cannot be activated by the eNB with the legacy UE. In this case the MME should determine a UP IP policy to be set to "not required".

**Legacy network nodes:**

An upgraded UE (to support UP IP), which establishes a new PDN connection with a legacy MME, UP IP cannot be activated by the eNB (even if the eNB supports UP IP).

**Mobility:**

At MME change (both at handover and idle mode mobility) a PDN connection with UP IP “required” shall be deactivated if UP IP is not supported by the target MME/target eNB or the new MME. At handover, if the source MME and the source eNB are upgraded to support UP IP, then the source MME/source eNB shall ensure that the PDN connection with activated UP IP due to a setting of UP IP to be “required” is not handed over to a target MME or a target eNB which does not support UP IP. At idle mode mobility, if the new MME is not upgraded to support UP IP, then PDN connection contexts with a setting of UP IP to be “required” shall not be forwarded from the old MME to the new MME.

### 6.11.5 Solution Evaluation

Editor's Note: write an evaluation of the solution against the relevant key issues here (or have an editor's note saying that it is to be added later.)

This solution meets the security requirement for key issue #1 (UP integrity activation in EPS) and impacts the UE, the MME, the LTE eNB and the HSS.

Currently the solution does not work when the UE and network nodes are of different releases, for example if a legacy UE wants to transfer data but the MME determines a UP IP policy to "required". If the configured operator policy allows the upgraded MME/eNB to handle the legacy UE, then in this case the MME should determine a UP IP policy to be set to "not required".

## 6.12 Solution #12: Using spare bit in existing 5G UE security capability to signal the UE support of UP IP over eUTRA to 5GC

### 6.12.1 Introduction

This solution addresses key issue #6 (UE connected to 5GC indicating support of UP IP over eUTRA).

This solution impacts the UE, the AMF and the ng-eNB.

### 6.12.2 Network options affected

This solution is applicable to the following network options:

- Option 4 - 5G core based Dual Connectivity (NR master - eUTRA secondary)

- Option 5 - 5G core with eUTRA

- Option 7 - 5G core based Dual Connectivity (eUTRA master - NR secondary)

### 6.12.3 Solution Description

The solution is to use one of the spare bits that is currently not used in 5G UE Security Capability IE (see clause 9.11.3.54 of TS 24.501 [10] copied below as Figure 6.12.3-1) to indicate that the UE supports user plane integrity protection with an ng-eNB. This would avoid taking one of the existing code points for indicating support/no support for encryption algorithms and integrity algorithms.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *8* | *7* | *6* | *5* | *4* | *3* | *2* | *1* |  |
| *UE security capability IEI* | | | | | | | | *octet 1* |
| *Length of UE security capability contents* | | | | | | | | *octet 2* |
| *5G-EA0* | *128-*  *5G-EA1* | *128-*  *5G-EA2* | *128-*  *5G-EA3* | *5G-EA4* | *5G-EA5* | *5G-EA6* | *5G-EA7* | *octet 3* |
| *5G-IA0* | *128-*  *5G-IA1* | *128-*  *5G-IA2* | *128-*  *5G-IA3* | *5G-IA4* | *5G-IA5* | *5G-IA6* | *5G-IA7* | *octet 4* |
| *EEA0* | *128-*  *EEA1* | *128-*  *EEA2* | *128-*  *EEA3* | *EEA4* | *EEA5* | *EEA6* | *EEA7* | *octet 5\** |
| *EIA0* | *128-*  *EIA1* | *128-*  *EIA2* | *128-*  *EIA3* | *EIA4* | *EIA5* | *EIA6* | *EIA7* | *octet 6\** |
| *0* | *0* | *0* | *0* | *0* | *0* | *0* | *0* |  |
| *Spare* | | | | | | | | *octet 7\* -10\** |

Figure 6.12.3-1: UE security capability information element

This information element is already protected to the core network in NAS signalling and also replayed to the UE to ensure Man-in-the-middle attacks are avoided.

This new spare bit would need to be signalled from the AMF to the RAN nodes and therefore mapped to a new information element on N2 interface. This new spare bit would also need to be signalled on the Xn interface between the RAN nodes and therefore mapped to a new information element on Xn interface.

At N2 handover with AMF re-allocation, the new spare bit would need to be signalled from the source AMF to the target AMF on N14 interface, mapped to a new information element.

At IW HO from 5GS to EPS and IW HO from EPS to 5GS, the new spare bit would be need to be signalled on N26 interface, mapped to a new information element.

The UE will always include the new spare bit in the following Registration Request message, as the UE security capability IE is always included in the Registration Request message at mobility when there is a possible AMF change.

### 6.12.4 Solution Evaluation

This solution meets the security requirement for key issue #6 (UE connected to 5GC indicating support of UP IP over eUTRA) and impacts the UE, the AMF and the ng-eNB.

It reuses the existing NAS signalling and the information element in a secure manner to indicate UE's support of user plane integrity protection over eUTRA to the network.

6.13 Solution #13: Using existing IEs to signal the UE support of UP IP over UTRA to EPC

6.13.1 Introduction

This solution addresses key issue #2 (Secure negotiation of integrity protection support in EPS).

This solution only impacts the UE and the eNB.

6.13.2 Network options affected

This solution is applicable to the following network options:

- Option 1 - eUTRA with EPC

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

6.13.3 Solution description

The solution is to use one of the bits that is used to indicate support of an EEA or EIA algorithm that is currently not used in the UE network capability IE and UE Security Capability IE (see clauses 9.9.3.34 and 9.9.3.36 of TS 24.301 [11] respectively) to indicate that the UE supports user plane integrity protection with an eNB.

This information element is already protected to the core network in NAS signalling and also replayed to the UE to ensure Man-in-the-middle attacks are avoided. It is also already signalled to the RAN nodes so would require no additional signalling.

6.13.4 Solution evaluation

This solution meets the security requirement for key issue #2 and only impacts the UE and the eNB as it reuses the existing NAS signalling and the information element in a secure manner to indicate UE's support of user plane integrity protection over eUTRA to the network.

## 6.14 Solution #14: LTE-EPC UP IP with option 3X/1X

### 6.14.1 Introduction

This solution uses NR PDCP in the EPS and UE to provide full rate User Plane Integrity Protection.

It is based on the capability of "Option 3" UEs to support NR PDCP (when used in the "option 3X" configuration), however the part of the UE's NR PDCP functionality used in an "option 3X" configuration may need to be extended to support NR UP IP capability. This solution would not change the UE's implementation of LTE PDCP.

NOTE: Other solutions may be proposed, e.g. that use User Plane Integrity Protection in LTE PDCP.

Within the network, the option 3X architecture the eNB can remotely control an entity implementing NR PDCP functionality.

With Release 17 RAN work (WID in RP-193181) on the Control Plane - User plane split of E-UTRAN, the architecture of option 1 will also allow the control plane of the eNB to remotely control an entity implementing PDCP functionality. As a deployment option, the network's PDCP functionality could be located at a gNB site (which uses NR-PDCP).

With the option 3X architecture, the UE's data radio bearers use NR-PDCP (specified in TS 38.323). The NR-PDCP firmware can be located in a separate gNB site, or in the "Centralised Unit" of a gNB implemented with a CU-DU split. This PDCP firmware can be common to what is used by the UE in "Option 2" operation and hence may be able to support User Plane Integrity Protection.

As specified in clause 4.2.2 of Release 15, TS 37.340:

*"In E-UTRA connected to EPC, if the UE supports EN-DC, regardless whether EN-DC is configured or not, the network can configure either E-UTRA PDCP or NR PDCP for MN terminated MCG bearers while NR PDCP is always used for all other bearers*."



Figure 6.14.1-1: Radio Protocol Architecture for MCG, SCG and split bearers from a UE perspective in MR-DC with EPC (EN-DC)

### 6.14.2 Network options affected

This solution is applicable to the following network options:

- Option 1 - eUTRA with EPC

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

### 6.14.3 Solution description

With the option 3X architecture, the UE's data radio bearers use NR-PDCP (specified in TS 38.323). The NR-PDCP firmware can be located in a separate gNB site, or in the "Centralised Unit" of a gNB implemented with a CU-DU split. This network PDCP firmware is what is expected to be used by "Option 2" UEs and hence can be expected to be able to support User Plane Integrity protection.

When configured to use EN-DC, the UE does not know whether the network will allocate radio resources on the NR cell, or the LTE cell, or both. The network allocates these resources dynamically - e.g. on a per TTI basis (1 ms on LTE, 500 ms (or less) on NR with 30 kHz subcarrier spacing). When resources are allocated on NR, the HARQ loop timings need to comply with the NR specifications, and these require faster processing times than on LTE. Hence the PDCP layer in an EN-DC UE needs to be adapted to work with NR speeds.

In Release 15, it is also perfectly feasible for the network to configure an EN-DC capable UE to use NR PDCP without the use of dual connectivity. This is specified in clause 4.2.2 of Release 15, TS 37.340 (copied below). Hence the addition of User Plane Integrity Protection in LTE could be realistic in, a UE that supports Option 2 UPIP.

*In E-UTRA connected to EPC, if the UE supports EN-DC, regardless whether EN-DC is configured or not, the network can configure either E-UTRA PDCP or NR PDCP for MN terminated MCG bearers while NR PDCP is always used for all other bearers.*



Figure 6.14.3-1: Radio Protocol Architecture for MCG, SCG and split bearers from a UE perspective in MR-DC with EPC (EN-DC)

Future changes to the UE's NR-PDCP firmware to support full rate option 2 NR UPIP may be able to be used by the UE with option 3(X) and hence also for option 1. The UE’s UPIP capabilities would be based on the NR algorithm options and would be signalled (to the MME) by adding 2 extra octets into the UE additional security capability IE defined in TS 24.301 clause 9.9.3.53 (by adding 2 octets, independent interoperability testing of the User Plane Integrity Protection for each of the NR PDCP algorithms is possible).

Editor's Note: The activation of UP security also needs to be described – whether it’s via AS SMC or RRC reconfiguration.

### 6.14.4 Solution Evaluation

Editor's Note: To be completed– extra aspects may still be identified.

This solution requires RAN upgrades and UE updates. Specifically, UE, MME, (and SGW and PGW) and RAN (S1 and e.g. X2) signalling software updates are expected. The UE PDCP layer needs to support FR UPIP.

NOTE: This solution requires UE to support NR-PDCP with the capability to run Integrity Protection at its full LTE data rate.

UE performance impact would be similar to that of NR devices, except that the lower data rates of LTE mean that the performance impact might well be less.

## 6.15 Solution #x: 'APN based control of UPIP usage'

### 6.15.1 Introduction

This solution addresses KI#8.

The solution uses the UE’s APN to resolve to a combined “PGW+SMF” in the HPLMN, and the 5GC PCF configures the PGW+SMF according to its existing 5GC behaviour. When the UE registers in EPC, the UPIP policy is downloaded in GTP-C signalling to the VPLMN’s EPC, and then sent in S1-AP signalling to the RAN.

### 6.15.2 Network options affected

This solution is applicable to the following network options:

- Option 1 - eUTRA with EPC

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

### 6.15.3 Solution Description

The solution is that the UE’s APN resolves to a combined “PGW+SMF” in the HPLMN, and the 5GC PCF configures the PGW+SMF according to its existing 5GC behaviour.

The GTP-C signalling from PGW to SGW to MME is extended to carry the “UPIP required/preferred/not needed” information to the MME. As GTP-C signalling largely operates on an EPS bearer basis rather than PDN connection basis, this signalling is sent on a per EPS-bearer basis.

Existing GTP-C signalling compatibility concepts are reused to enable the PGW and SGW to have prior knowledge as to whether the SGW and MME support this “UPIP required/preferred/not needed” signalling. Hence the PGW can block the establishment of EPS bearers on MMEs that do not support UPIP “policing”.

The UE’s support (or not) for Full Rate UPIP is signalled from the UE to the MME.

The MME uses the “UPIP required/preferred/not needed” information from the PGW and the UE’s support for FR-UPIP to determine what EPS bearers are permitted to be established when the UE performs a Service Request (or Attach, PDN Connectivity Request or Dedicated Bearer Activation occurs).

For those bearers that pass this check, the MME signals the “UPIP required/preferred/not needed” information to the eNB in R17 extensions of S1-AP signalling that:

1. allow the UPIP “Preferred” and “Not-needed” settings to be ignored by a non-supporting eNB, and

b) ensure that the UPIP “Required” setting causes a non-supporting eNB to reject the request. (This procedure might be enhanced by UPIP-supporting eNBs indicating their support in the S1 Setup message).

Using similar message encoding techniques, at S1 handover (including 5GC to EPC handover), the ‘source to target transparent container’ is used to signal the “UPIP required/preferred/not needed” information to the target eNB.

At X2 handover, X2-AP signalling extensions carry the “UPIP required/preferred/not needed” information to the target eNB using similar message encoding techniques.

NOTE 1: Use of the above message encoding within the S1 interface transparent container enables “UPIP Required” enforcement at inter-MME handover (and 5GC to EPC handover) to a target MME that does not support UPIP policing.

NOTE 2: To restore UPIP usage (when “Preferred”) after S1/X2 handovers from a non-supporting eNB to a supporting eNB, the MME inserts the “UPIP required/preferred/not needed” information into the S1-AP Handover Command (S1 case) and Path Switch Request Ack (X2 case) messages.

NOTE 3: Use of “UPIP Required” is not recommended unless the HPLMN is confident that the UE will only move within areas where there is full VPLMN support for UPIP.

NOTE 4: The PGW is not aware of the UE’s support (or not) for FR UPIP on EPC. The PGW does not need to be aware of the UE’s support level because the ‘UPIP policing’ function has to be performed in the MME and not in the PGW+SMF. This is because (in contrast to 5GC), EPS procedures such as Service Request need only involve the MME and need not involve the PGW+SMF.

NOTE 5: As described in solution #14, with Release 17 RAN work (WID in RP-193181) on the Control Plane - User plane split of E-UTRAN, the architecture of option 1 will also allow the control plane of the eNB to remotely control an entity implementing PDCP functionality. As a deployment option, the network's PDCP functionality could be located at a gNB site (which uses NR-PDCP).

### 6.15.4 Solution Evaluation

Editor's Note: To be completed.

## 6.16 Solution #16: Use existing behaviour to block transfer to EPS of PDN connections that have UPIP set to “Required”

### 6.16.1 Introduction

This solution addresses key issue #7 (Ensuring UP IP is enforced at interworking).

This solution has no impact on any node.

### 6.16.2 Network options affected

This solution is applicable to the following network options:

- Option 1 - eUTRA with EPC

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

### 6.16.3 Solution description

The solution proposes to keep the existing procedures for not passing bearers that require UP IP to EPS. This ensures that no bearer that requires UP IP is ever used without UP IP.

### 6.16.4 Solution evaluation

The solution has no impact to any nodes but comes at the cost of not being able to move bearers that require UP IP to EPS. For a UE with UPIP set to Required for all its PDN connections (and an MME that does not support “attach without PDN connectivity”), the NG-RAN would keep the UE connection until it suffers radio link failure and therefore cause extra interference into adjacent LTE cells. This is an issue of existing behaviour and not introduced by this solution.

## 6.x Solution #x: 'Title of solution'

### 6.x.1 Introduction

Editor's Note: give an overview of the solution making sure that you identify which key issues are being addressed in this solution.

Editor's Note: please identify the network elements and interfaces affected by the solution.

### 6.x.2 Network options affected

This solution is applicable to the following network options:

- Option 1 - eUTRA with EPC

- Option 2 - NR standalone with 5G Core

- Option 3 - EPC based Dual Connectivity of eUTRA and NR RAT

- Option 4 - 5G core based Dual Connectivity (NR master - eUTRA secondary)

- Option 5 - 5G core with eUTRA

- Option 7 - 5G core based Dual Connectivity (eUTRA master - NR secondary)

Editor's note: delete the ones that are not applicable.

### 6.x.3 Solution Description

Editor's Note: describe the solution in detail here

### 6.x.4 Solution Evaluation

Editor's Note: write an evaluation of the solution against the relevant key issues here (or have an editor's note saying that it is to be added later.)

# 7 Conclusions

## 7.1 Conclusions on UE connects to 5GC via eUTRA

It is concluded that the Rel-15 architectural approach of applying user plane integrity protection at NR PDCP layer in TS 33.501 is adopted as the basis for normative work for the following network options:

- Option 2 - NR standalone with 5G Core

- Option 4 - 5G Core based Dual Connectivity (NR master - eUTRA secondary)

- Option 5 - 5G Core with eUTRA

- Option 7 - 5G Core based Dual Connectivity (eUTRA master - NR secondary)

For Key Issue #6 (UE connected to 5GC indicating support of UP IP over eUTRA), Solution #8 (Using existing 5G UE security capability to signal the UE support of UP IP over eUTRA to 5GC) is adopted for the normative work.

Editor's Note: Further conclusion(s) are FFS.

## 7.2 Conclusions on UE connects to EPC via eUTRA

Editor's Note: This clause will capture the conclusions on activating UP IP when UE connects to EPC via eUTRA.

# 8 Recommendations

Editor's Note: This clause will contain any recommendations for further work

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **Tdoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2019-01 | SA3#94 | S3-190006 | - | - | - | First draft | 0.0.1 |
| 2019-01 | SA3#94 | S3-190550 | - | - | - | Added S3-190015, S3-190101 and S3-190551 | 0.1.0 |
| 2019-03 | SA3#94AH | S3-190910 | - | - | - | Added S3-190647, S3-190914, S3-191019 and S3-191004 | 0.2.0 |
| 2019-05 | SA3#95 | S3-191775 | - | - | - | Added S3-191263, S3-191543 and S3-191776 | 0.3.0 |
| 2019-06 | SA3#95bis | S3-192424 | - | - | - | Added S3-192423, S3-192426, S3-192422, S3-192425 and S3-192455 | 0.4.0 |
| 2019-08 | SA3#96 | S3-193147 | - | - | - | Added S3-193143, S3-193144, S3-193145 and S3-193146 | 0.5.0 |
| 2019-20 | SA3#96ah | S3-193693 | - | - | - | Added S3-193691, S3-193698, S3-193692, S3-193694, S3-193578, S3-193697, S3-193696, S3-193695 | 0.6.0 |
| 2019-11 | SA3#97 | S3-194672 | - | - | - | Added S3‑194698, S3‑194671, S3‑194121 and S3‑194289, | 0.7.0 |
| 2020-04 | SA98bis | S3-200804 | - | - | - | Added S3-200611, S3-200832, S3-200833, S3-200761, S3-200768 and | 0.8.0 |
| 2020-05 | SA3#99 | S3-201430 | - | - | - | Added S3-201366, S3-201427 and S3-201421 | 0.9.0 |
| 2020-06 | SA#88-e | SP-200377 |  |  |  | MCC and EditHelp review  Presented for information and approval | 1.0.0 |
| 2020-08 | SA#100e | S3-202260 | - | - | - | Added S3-202257, S3-202045, S3-202258,S3-202097, S3-202086 and S3‑201957. | 1.1.0 |