3GPP TR 33.825 V16.0.1 (2019-10)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Study on the security of Ultra-Reliable Low-Latency Communication (URLLC) for the 5G System (5GS)

(Release 16)

** 

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

Keywords

5G, security, URLLCC

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

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

Internet

http://www.3gpp.org

***Copyright Notification***

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

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

All rights reserved.

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

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

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

Contents

Foreword [5](#__RefHeading___Toc22565074)

1 Scope [7](#__RefHeading___Toc22565075)

2 References [7](#__RefHeading___Toc22565076)

3 Definitions of terms, symbols and abbreviations [7](#__RefHeading___Toc22565077)

3.1 Terms [7](#__RefHeading___Toc22565078)

3.2 Symbols [7](#__RefHeading___Toc22565079)

3.3 Abbreviations [8](#__RefHeading___Toc22565080)

4 Security aspects of 5G URLLC [8](#__RefHeading___Toc22565081)

5 Key issues [8](#__RefHeading___Toc22565082)

5.1 Key Issue #1: Security for redundant transmission [8](#__RefHeading___Toc22565083)

5.1.1 Key issue details [8](#__RefHeading___Toc22565084)

5.1.2 Security threats [9](#__RefHeading___Toc22565085)

5.1.3 Potential Security requirements [9](#__RefHeading___Toc22565086)

5.2 Key issue #2: Support of security for high reliability by redundant data transmission in user plane [9](#__RefHeading___Toc22565087)

5.2.1 Key issue details [9](#__RefHeading___Toc22565088)

5.2.2 Security threats [10](#__RefHeading___Toc22565089)

5.2.3 Potential security requirements [10](#__RefHeading___Toc22565090)

5.3 Key Issue #3: UP security policy handling for multiple PDU sessions established for redundant data transmission [10](#__RefHeading___Toc22565091)

5.3.1 Key issue details [10](#__RefHeading___Toc22565092)

5.3.2 Security threats [11](#__RefHeading___Toc22565093)

5.3.3 Potential security requirements [11](#__RefHeading___Toc22565094)

5.4 Key Issue #4: Security policy for URLLC service [11](#__RefHeading___Toc22565095)

5.4.1 Key issue details [11](#__RefHeading___Toc22565096)

5.4.2 Security threats [11](#__RefHeading___Toc22565097)

5.4.3 Potential Security requirements [12](#__RefHeading___Toc22565098)

5.5 Key Issue #5: Security aspect of low latency handover procedure [12](#__RefHeading___Toc22565099)

5.5.1 Key issue details [12](#__RefHeading___Toc22565100)

5.5.2 Security threats [12](#__RefHeading___Toc22565101)

5.5.3 Potential Security requirements [12](#__RefHeading___Toc22565102)

5.6 Key Issue #6: Retaining AS security keys for redundant data transmission in user plane [12](#__RefHeading___Toc22565103)

5.6.1 Key issue details [12](#__RefHeading___Toc22565104)

5.6.2 Security threats [13](#__RefHeading___Toc22565105)

5.6.3 Potential security requirements [13](#__RefHeading___Toc22565106)

5.7 Key Issue #7: QoS monitoring protection [13](#__RefHeading___Toc22565107)

5.7.1 Key issue details [13](#__RefHeading___Toc22565108)

5.7.2 Security threats [13](#__RefHeading___Toc22565109)

5.7.3 Potential Security requirements [13](#__RefHeading___Toc22565110)

5.8 Key Issue #8: Acceleration of authentication and key agreement procedure for low latency [13](#__RefHeading___Toc22565111)

5.8.1 Key issue details [13](#__RefHeading___Toc22565112)

5.8.2 Security threats [13](#__RefHeading___Toc22565113)

5.8.3 Potential Security requirements [13](#__RefHeading___Toc22565114)

5.9 Key Issue #9: Security aspect of low latency Re-authentication procedure [14](#__RefHeading___Toc22565115)

5.9.1 Key issue details [14](#__RefHeading___Toc22565116)

5.9.2 Security threats [14](#__RefHeading___Toc22565117)

5.9.3 Potential security requirements [14](#__RefHeading___Toc22565118)

5.10 Key Issue #10: UP security performance for low latency [14](#__RefHeading___Toc22565119)

5.10.1 Key issue details [14](#__RefHeading___Toc22565120)

5.10.2 Security threats [14](#__RefHeading___Toc22565121)

5.10.3 Potential Security requirements [14](#__RefHeading___Toc22565122)

6 Candidate Solutions [15](#__RefHeading___Toc22565123)

6.1 Solution #1: Security solution for handling UP security policy for multiple PDU sessions for redundant data transmission [15](#__RefHeading___Toc22565124)

6.1.1 Introduction [15](#__RefHeading___Toc22565125)

6.1.2 Solution details [15](#__RefHeading___Toc22565126)

6.1.3 Evaluation [16](#__RefHeading___Toc22565127)

6.2 Solution #2: Retaining AS security keys for redundant data transmission in user plane [16](#__RefHeading___Toc22565128)

6.2.1 Introduction [16](#__RefHeading___Toc22565129)

6.2.2 Solution details [16](#__RefHeading___Toc22565130)

6.2.3 Evaluation [16](#__RefHeading___Toc22565131)

6.3 Solution #3: Security policy handling for redundant data transmission [16](#__RefHeading___Toc22565132)

6.3.1 Introduction [16](#__RefHeading___Toc22565133)

6.3.2 Solution details [17](#__RefHeading___Toc22565134)

6.3.3 Evaluation [18](#__RefHeading___Toc22565135)

6.4 Solution #4: Security support for N3 tunnel redundancy [18](#__RefHeading___Toc22565136)

6.4.1 Introduction [18](#__RefHeading___Toc22565137)

6.4.2 Solution details [18](#__RefHeading___Toc22565138)

6.4.3 Evaluation [19](#__RefHeading___Toc22565139)

6.5 Solution #5: Security for redundant data transmission [19](#__RefHeading___Toc22565140)

6.5.1 Introduction [19](#__RefHeading___Toc22565141)

6.5.2 Solution details [19](#__RefHeading___Toc22565142)

6.5.3 Evaluation [20](#__RefHeading___Toc22565143)

6.7 Solution #7: Security for redundant data transmission using Dual Connectivity [21](#__RefHeading___Toc22565144)

6.7.1 Introduction [21](#__RefHeading___Toc22565145)

6.7.2 Solution details [22](#__RefHeading___Toc22565146)

6.7.3 Evaluation [23](#__RefHeading___Toc22565147)

6.8 Solution #8: Handling of UP security activation status and selection of SN in Dual Connectivity [24](#__RefHeading___Toc22565148)

6.8.1 Introduction [24](#__RefHeading___Toc22565149)

6.8.2 Solution details [24](#__RefHeading___Toc22565150)

6.8.3 Evaluation [26](#__RefHeading___Toc22565151)

7 Conclusions [26](#__RefHeading___Toc22565152)

7.1 Key Issue #1: Security for redundant transmission [27](#__RefHeading___Toc22565153)

7.2 Key Issue #2: Support of security for high reliability by redundant data transmission in user plane [27](#__RefHeading___Toc22565154)

7.3 Key Issue #3: UP security policy handling for multiple PDU sessions established for redundant data transmission [28](#__RefHeading___Toc22565155)

7.4 Key Issue #4: Security policy for URLLC service [28](#__RefHeading___Toc22565156)

7.6 Key Issue #6: Retaining AS security keys for redundant data transmission in user plane [28](#__RefHeading___Toc22565157)

7.8 Key Issue #8: Acceleration of authentication and key agreement procedure for low latency [28](#__RefHeading___Toc22565158)

Annex A: Change history [29](#__RefHeading___Toc22565159)

# 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.

# 1 Scope

The present document:

- Investigates and identifies the security key issues for meeting the low latency requirement.

- Investigates and identifies the security key issues for meeting the ultra-high reliability requirement.

- Provides potential security requirements to address the identified security issues.

- Provides the potential security solutions to support URLLC services.

# 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 TR 23.725 "Study on enhancement of Ultra-Reliable Low-Latency Communication (URLLC) support in the 5G Core network".

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

[4] 3GPP TS 23.501: "System Architecture for the 5G System".

[5] 3GPP TS 23.502: "Procedures for the 5G System".

[6] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[7] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[8] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[9] 3GPP TS 37.340: "NR; Multi-connectivity; Overall description; Stage-2".

[10] 3GPP TS 23.503: "Policy and charging control framework 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].

DC Dual Connectivity

MCG Master Cell Group

MgNB Master gNB

MN Master Node

NG-RAN Next Generation-RAN

NR New Radio

NR-DC NR-NR Dual Connectivity

PDU Packet Data Unit

PDCP Packet Data Convergence Protocol

SCG Secondary Cell Group

SgNB Secondary gNB

S-RAN Secondary RAN

SN Secondary Node

UP User Plane

URLLC Ultra-Reliable Low-Latency Communication

# 4 Security aspects of 5G URLLC

The 5GS defined in TS 23.501 [4] is used as the baseline network architecture for 5G URLLC. URLLC needs to support both high reliability and low latency. In order to ensure the high reliability, redundant transmission in 5GS is supported on multiple user plane data paths, something that can hardly be achieved by single path on user plane. Accordingly, the applicable security mechanisms for supporting redundant transmission cover all aspect of the communication, including PDU session establishment, handover etc. As for low latency aspect, the other important requirements for URLLC as described in TR 23.725 [2] include QoS Monitoring to assist URLLC service and optimization for handover procedure, both of which are addressed. The security considerations in this case are covered as well. Moreover, additional security aspects of control plane or user plane optimizations for ensuring the high reliability and reducing latency are also considered together during the whole study and are reflected in the present document.

# 5 Key issues

## 5.1 Key Issue #1: Security for redundant transmission

### 5.1.1 Key issue details

This key issue addresses the security aspects of key issue #1: Supporting high reliability by redundant transmission in user plane in TR 23.725 [2].

According to the TR 23.725 [2], in order to ensure the high reliability which can hardly be achieved by single path on user plane, redundant data transmission in 5GS may be supported. In this case it is important to study how to ensure that these redundant transmissions are secure enough. From security perspective, repeated user plane data transmission may introduce new security risks. Redundant transmission, where the data is duplicated at the source and sent to the destination over two different paths, may increase the security risk when the two received transmissions are not identical. Therefore, the receiver cannot know which of the transmissions is correct.

TR 23.725 [2] recommends solution #1 "Redundant user plane paths based on dual connectivity" and solution #4 "Supporting redundant data transmission via single UPF and single RAN node" to resolve key issue #1 in TR 23.725 [2]. Solution #1 is based upon the Dual Connectivity (DC) feature. Two PDU sessions will be established in this solution for redundant data transmission, where one PDU session uses a MCG bearer via the Master gNB, and the second PDU session uses a SCG bearer via the Secondary gNB in the user plane. The architecture is as follows:



Figure 5.1.1-1: Architecture for redundant UP paths for URLLC using Dual Connectivity

Solution #3 recommends that the redundant packets will be transferred via two independent N3 tunnels between a single NG-RAN node and the UPF, which are associated with a single PDU Session, over different transport layer path to enhance the reliability of service. The NG-RAN node and UPF support the packet replication and elimination function.



Figure 5.1.1-2: Architecture for Redundant transmission with two N3 tunnels between the UPF and a single NG-RAN node

### 5.1.2 Security threats

The attacker can monitor the data streams and may identify if a data stream is re-used. It is possible for the attacker to link two data streams used for redundant data transmission. The attacker could use such information in its advantage to mount targeted attacks against radio bearers or N3 tunnels serving URLLC PDU sessions if the corresponding radio bears or N3 tunnels are not integrity, encryption and replay protected.

### 5.1.3 Potential Security requirements

The 5G system shall provide an appropriate security method to protect the redundant transmission.

The system shall provide cryptographic separation for radio bearers serving redundant transmissions.

The added paths for redundancy shall provide equal level of security compared to single path.

## 5.2 Key issue #2: Support of security for high reliability by redundant data transmission in user plane

### 5.2.1 Key issue details

There have been discussions in SA2 on architectural aspect of the 5GS to support high reliability in the UP by introducing multiple redundant transmission paths, where the UP bearer is transferred over multiple paths via 2 different gNBs and UPFs (Solution #1, #2). For this redundant UP bearer transmission, security aspects such as confidentiality protection, integrity protection, and key handling, need to be considered in SA3.

### 5.2.2 Security threats

Having multiple paths for the UP, in effect, introduces additional threat surface for attackers to take advantage of. In order to realize high level of reliability in communication by using redundant UP paths, security of both UP paths need to be protected equally. Having one of the two UP paths compromised implies the whole proposition of URLLC collapses. Therefore, appropriate security solution for redundant transmission via multiple paths in the UP need to be in place.

### 5.2.3 Potential security requirements

Confidentiality protection over the air shall be supported for UP data via redundant multiple transmission paths.

Integrity protection over the air shall be supported for UP data via redundant multiple transmission paths.

## 5.3 Key Issue #3: UP security policy handling for multiple PDU sessions established for redundant data transmission

### 5.3.1 Key issue details

This key issue addresses the security aspects of key issue #1: Supporting high reliability by redundant transmission in user plane in SA2 TR 23.725 [2].

According to the SA2 TR 23.725 [2], in order to ensure the high reliability which can hardly be achieved by single path on user plane, redundant transmission in 5GS may be supported. Depending on the condition of network deployment, e.g., which NFs or segments cannot meet the requirements of reliability, the redundant transmission may be applied on the user plane path between the UE and the network.

There are several potential solutions in SA2 TR 23.725 [2], where redundant data transmission in user plane takes different paths.

During the PDU session establishment, the 5G Core Network should determine and provide the UP security policy for a PDU session to the gNB connected to 5GC according to TS 23.501 [4] and TS 23.502 [5].

The 5G Core Network may enforce different configurations of UP security (encryption and integrity protection) in the UP security policy for multiple PDU sessions established for redundant data transmission.

The UPF or the DN has no knowledge of which UP security policy that has been applied between the UE and the gNB for the redundant user plane data transmission that has taken different paths. TR 23.725 [2] recommends solution #1 "Redundant user plane paths based on dual connectivity" to resolve key issue #1 in TR 23.725 [2]. This solution is based upon the Dual Connectivity (DC) feature. Two PDU sessions will be established in this solution for redundant data transmission, where one PDU session uses a MCG bearer via the Master gNB, and the second PDU session uses a SCG bearer via the Secondary gNB in the user plane. Based on theses PDU sessions, two independent paths are setup. UPF1 and UPF 2 are connect to the same Data Network (DN).



Figure 5.3.1-1: Architecture for redundant User Plane paths for URLLC using Dual Connectivity

### 5.3.2 Security threats

If the attacker knows that integrity protection is enabled on one path but not on a second path, then the attacker could perform jamming on the first path in order to prevent the user plane data to be forwarded from the gNB to the UPF, and at then modify user plane data sent over the second path.

### 5.3.3 Potential security requirements

If encryption of user plane data is enabled between the UE and the gNB on the first path for a first PDU session, then encryption shall be enabled for redundant user data transmission over a second path for a second PDU session as well.

If integrity protection of user plane data is enabled between the UE and the gNB on the first path for a first PDU session, then integrity protection shall be enabled for redundant user data transmission over a second path for a second PDU session as well.

When Dual Connectivity is used, the MgNB shall ensure that the UP security policy assigned to the MgNB is forwarded and used by the SgNB for the two PDU Sessions used for redundant data transmission.

## 5.4 Key Issue #4: Security policy for URLLC service

### 5.4.1 Key issue details

The URLLC service scenarios include both the high reliability and low latency requirements. From security perspective, there is a tight coupling between ultra-reliable and low latency to maintain the same level of security and be efficient in doing so at the same time, the former implies need for stringent security checks, while the latter may imply extremely fast security checks. Hence, in the URLLC services there may be a need for various security policies, e.g., for length of key refreshment interval, the recommended length of keys, etc.

One example of an area where policies may be needed is the User Plane Security. In 5GS, a new security feature was introduced: the User Plane Security Policy. The SMF will get User Plane Security Policy during PDU Session Establishment from UDM and PCF. The SMF generates User Plane Security Enforcement and transfers it to the RAN. The Release 15 RAN can only apply integrity protection in low speed (maximum of 64 kbps). For URLLC service with higher speed than 65 kbps, the RAN cannot fulfil the QoS requirement while enforcing user plane integrity protection. The confidentiality protection may additionally bring x ms (e.g. 0.1~2 ms depending the implementation) delay. This delay may have negative impact on URLLC services. Having different policies for different services may help with these issues.

### 5.4.2 Security threats

If the URLLC service is not user plane integrity protected, the user data can be modified during the transmission. On the other hand, after adding integrity protection, the delay may be unacceptable for some URLLC services. If service-specific security policies are not applied, there may be a risk that many URLLC services have insufficient protection.

### 5.4.3 Potential Security requirements

The 5G system shall provide a user plane security policy mechanism applicable to URLLC services.

The 5G system shall provide the mechanism for how to enforce User Plane Security Policy when there are URLLC services in the PDU Session.

The selection of the security policy shall be under network control.

## 5.5 Key Issue #5: Security aspect of low latency handover procedure

### 5.5.1 Key issue details

In order to guarantee low latency to the URLLC services, according to TR 23.725 [2], the optimization of handover procedure is needed. However, the security handling in handover, e.g. key derivation, security algorithm selection should be considered at the same time in order to support handover in URLLC. For URLLC services that require the low latency performance, security should not be reduced. Optimization of handover procedure in this case should maintain the same level of security as in other 5G services.

### 5.5.2 Security threats

If the interfaces e.g. N2 are not security protected, then an attacker could eavesdrop or insert or modify the security key and the security parameters transferred on the interface.

If the target AMF is compromised and the UE security keys do not have the property of backward security, then an attacker would be able to decrypt the previous data exchanged between the UE and the network. If the source AMF is compromised and the UE security keys do not have the property of forward security, then an attacker would be able to decrypt the future data exchanged between the UE and the network.

If the AMF is compromised, it may purposefully bid down the algorithm to a lower priority algorithm that is fairly easier to crack. This is also applicable when a MiTM masquerades the connection.

### 5.5.3 Potential Security requirements

The 5G system shall provide the proper security protection for the optimized URLLC handover procedure.

## 5.6 Key Issue #6: Retaining AS security keys for redundant data transmission in user plane

### 5.6.1 Key issue details

This key issue addresses the security aspects of key issue #1: Supporting high reliability by redundant transmission in user plane in SA2 TR 23.725 [2] and key issue #2: Supporting high reliability by redundant transmission in user plane.

The flexibility to retain or to change the AS security keys in the gNB in intra-gNB handover i.e. between cells belonging to the same gNB, was introduced in 5G system in TS 33.501 [3] Rel-15 clause 6.9.2.3.1.

If AS keys are always refreshed even when not required, then performance in gNB could be degraded. Refreshing the AS keys have impact on performance as time delay. To support services with very strict performance requirements, e.g. low latency or high reliability, would clearly benefit from avoiding unnecessary AS keys to be refreshed. The gNB should only refresh the AS security keys when there are security reasons.

URLLC services should be taken into considerations when performing the configuration of the policy for controlling when to retain or change AS keys in gNB.

### 5.6.2 Security threats

N/A

### 5.6.3 Potential security requirements

N/A

## 5.7 Key Issue #7: QoS monitoring protection

### 5.7.1 Key issue details

Since the vertical applications may want to be aware of the real time latency, the 5G E2E QoS monitoring is used to monitor the real time packet delay in 5GC and 5G-AN. According to TR23.725 [2], it is possible to define the new procedures and functions on QoS monitoring activation and enforcement. In this case, these monitoring messages are required to be protected. Furthermore, whether the related interfaces need to be security protected is also necessary to be considered.

### 5.7.2 Security threats

In lack of a secure way of protecting the E2E QoS monitoring procedure, an attacker could perform to modify the packet or message to obtain the incorrect latency report.

### 5.7.3 Potential Security requirements

The 5G system shall be able to protect the 5G E2E QoS Enforcement procedure for a service.

## 5.8 Key Issue #8: Acceleration of authentication and key agreement procedure for low latency

### 5.8.1 Key issue details

NOTE: The re-authentication enhancement is irrelevant to URLLC services which is for UP traffic.

The R15 authentication and key agreement (AKA) procedure always involves HPLMN (i.e. AUSF and UDM) to query new AV from HPLMN and authenticate the UE by HPLMN. The NAS SMC procedure also is a part of the AKA procedure in R15, which is used to verify KSEAF is generated correctly both in UE and network. It is less efficient compared to AKA procedure in LTE, but increase security for home control and identifier privacy.

It needs to be studied that how to enhance the AKA procedure to reduce the latency to authenticate the UE and setup new security context for the UE without downgrading the security level of R15 AKA procedure, and which node of the visited network can be the network endpoint of the enhanced AKA procedure.

### 5.8.2 Security threats

N/A.

### 5.8.3 Potential Security requirements

N/A.

## 5.9 Key Issue #9: Security aspect of low latency Re-authentication procedure

### 5.9.1 Key issue details

NOTE: The re-authentication enhancement is irrelevant to URLLC services which is for UP traffic.

In order to guarantee low latency to the URLLC services, according to TR 23.725 [2], a fast re-authentication procedure may be considered. Where the TS 33.501 [3] clause F.1 states that, the fast re-authentication is not supported in 5GS. In this case, a time consuming authentication procedure need to be invoked for every registration request from a UE irrespective of their previous authentication with a same network.This may have a significant impact over the URLLC services.

Time consuming authentication procedure irrespective of a UE's previous authentication may lead to URLLC service failure.

### 5.9.2 Security threats

No security threat.

### 5.9.3 Potential security requirements

TBA.

## 5.10 Key Issue #10: UP security performance for low latency

### 5.10.1 Key issue details

The low latency service has extreme requirements on UP data transmitting delay. Without security, data transmitting is very quick using nowadays technology. Introducing of security in UP data transmitting will delay the data transmitting, but it is a trade-off between performance and security.

The UP path between UE and UPF includes radio interface and N3 interface, and may include F1 interface (DU-CU case) and Xn (handover case) interface.

In current specification, IPsec protocol may be used to protect above interfaces. It has been identified that IPsec and TLS/DTLS will slow down the data forwarding performance significantly, which means UP data transmitting over above interfaces will be delayed significantly if IPsec is deployed.

It has been identified that security performance on radio interface also is able to be improved, e.g. by using AES GCM mode.

NOTE: The justification on low latency for UP traffic for URLLC services is needed.

### 5.10.2 Security threats

TBD.

### 5.10.3 Potential Security requirements

TBD.

# 6 Candidate Solutions

## 6.1 Solution #1: Security solution for handling UP security policy for multiple PDU sessions for redundant data transmission

### 6.1.1 Introduction

This solution addresses key issue #3: UP security policy handling for multiple PDU sessions established for redundant data transmission.

According to TS 23.501 [4] and TS 23.502 [5], the SMF should determine and provide the UP security policy for a PDU session to the gNB connected to 5GC during the PDU session establishment procedure.

The UP security policy should indicate whether UP confidentiality and/or UP integrity protection shall be activated or not for all DRBs belonging to that PDU session. The UP security policy should be used by gNB to activate UP confidentiality and/or UP integrity for all DRBs belonging to the PDU session.

According to TS 23.501 [4], the User Plane Security Policy provides the same level of information than User Plane Security Enforcement information. Once the User Plane Security Enforcement information is determined at the establishment of the PDU Session, it is provided to the UE and applies for the life time of the PDU Session. The User Plane Security Enforcement information provides the NG-RAN with User Plane security policies for a PDU session. It indicates:

- whether UP integrity protection is:

- Required: for all the traffic on the PDU Session UP integrity protection shall apply.

- Preferred: for all the traffic on the PDU Session UP integrity protection should apply.

- Not Needed: UP integrity protection shall not apply on the PDU Session.

- whether UP confidentiality protection is:

- Required: for all the traffic on the PDU Session UP confidentiality protection shall apply.

- Preferred: for all the traffic on the PDU Session UP confidentiality protection should apply.

- Not Needed: UP confidentiality shall not apply on the PDU Session.

### 6.1.2 Solution details

The User Plane Security Policy for multiple PDU Sessions used for redundant data transmission should have the same setting for encryption and for integrity protection. The gNB should not be allowed to override the UP Security Policy received from the 5G Core Network. The setting defined in clause 5.10.3 TS 23.501 [4] should apply with the following modifications:

- Encryption:

- only "Required" or "Not Needed" is allowed;

- "Preferred" is not allowed:

- Integrity protection:

- only "Required" or "Not Needed" is allowed;

- "Preferred" is not allowed:

In addition, if redundant data transmission is taking place over E-UTRA (connected to 5GC), then the setting of "Required" for Integrity protection is not allowed.

When Dual Connectivity as described in Figured 5.3.1-1 of the KI #3 is used, both of the two redundant PDU sessions are initially established via the MgNB. The SMF shall provide two UP security policies for each of the two redundant PDU sessions to the MgNB during the PDU sessions establishment procedure, if SMF recognizes one of the UP security policies is not the same as the other one, the SMF shall modify the UP security policies to make sure them to be same.

However, MgNB shall ensure that the two redundant PDU sessions have the same UP integrity and encryption activation after the MgNB receives UP security policy and proceeds according to TS 33.501 [3] clause 6.6.1.

### 6.1.3 Evaluation

The proposed solution needs to modify the existing UP security policy definition as specified in TS 23.501 [4] which is provided to the NG-RAN by SMF for a PDU session. The modification is specific for URLLC services. For DC architecture used for URLLC service, the solution is applicable if the UP security policies which are used by Master node and Secondary node for redundant PDU session transmissions are the same.

Based on above analysis of the proposed solution, the solution is able to meet the potential security requirements of KI #3.

## 6.2 Solution #2: Retaining AS security keys for redundant data transmission in user plane

### 6.2.1 Introduction

This solution address Key Issue #6: Retaining AS security keys for redundant data transmission in user plane

### 6.2.2 Solution details

The flexibility to retain or to change the AS security keys in the gNB in intra-gNB-CU handover i.e. between cells belonging to the same gNB, was introduced in 5G system in TS 33.501 [3] clause 6.9.2.3.1 Intra-gNB-CU handover.

It is proposed to re-use the existing solution as specified in TS 33.501 [3] clause 6.9.2.3.1 Intra-gNB-CU handover (about the policy for controlling) when to retain or change AS keys in gNB when URLLC services are used.

When the DC architecture as specified in KI#3 is used for redundant data transmission data, if the current KgNB in MgNB is changed because of intra-gNB-CU handover, the MgNB shall update the security key which are used to protect the two redundant PDU sessions as described in TS 33.501 [3].

### 6.2.3 Evaluation

The proposed solution fulfils the potential security requirements of KI#6.

## 6.3 Solution #3: Security policy handling for redundant data transmission

### 6.3.1 Introduction

This solution addresses Key Issue#3 and Key Issue#4 by identifying how to handle the security policy for redundant transmission. In this solution, it is assumed that the redundant transmissions are established by two independent paths which require two RAN nodes and two UPFs to a single UE. This solution is based on the following architecture (see TR 23.725 [2] v0.4.0 clause 6.1):



Figure 6.3.1-1: redundant transmission architecture

This architecture is based on Dual Connectivity architecture, except that there are two UPFs.

According to the figure above, if there are two PDU sessions that take two different user plane paths which are used to transfer the redundant data, the security policy for the redundant PDU sessions shall be ensured to be the same.

### 6.3.2 Solution details

If the high-reliability is fulfilled by redundant transmission based on NR-DC architecture, the following user plane security policy mechanism shall apply:

In case where one of the redundant PDU Session data transmissions is terminated at the MgNB and the other one is terminated at the SgNB, these two redundant data transmissions shall have the same UP integrity protection and ciphering policy. In addition, the MgNB shall inform the SgNB with its UP integrity protection and encryption activation decision of the PDU Session which is terminated at MgNB but is redundant with the other PDU Session terminated at the SgNB.

MgNB shall make the decision on UP encryption protection and integrity protection according to the UP security policy for these two redundant transmissions. The MgNB shall inform the SgNB the encryption protection and integrity protection indications of the transmission terminated at itself via SgNB Addition/Modification Request message during when the corresponding redundant transmission is moved to SgNB. At the reception of the indications, the SgNB shall attempt to comply with the request from MgNB to ensure these two UP ciphering protection indications are the same.

If the UP security policy indicates UP integrity protection "Not needed", the UP integrity protection shall not be applied on the two redundant PDU sessions and the MgNB informs the decision to SgNB, in other words, UP integrity protection shall not be activated for the two redundant PDU sessions. If the UP security policy indicates UP encryption protection "Not needed", the MgNB shall have the encryption protection either "off", and inform the decision to SgNB. If the UP security policy indicates UP encryption protection "preferred", the MgNB shall have the encryption protection either "on" or "off", and inform the decision to SgNB.

Particularly, in case of the MgNB cannot activate UP confidentiality and/or integrity when the received UP security policy is "Required" or "Preferred", the MgNB shall reject establishment of UP resources for the PDU Session and indicate the decision to the SgNB in order to make sure these two redundant transmissions have the same UP encryption protection and integrity protection.

In all cases, the SgNB shall inform the UP integrity protection and encryption indications to the MgNB in the SgNB Addition/Modification Request Acknowledgement message. The MgNB shall forward the UP integrity protection and encryption indications to the UE in RRC Connection Reconfiguration message.

In addition, if the UP integrity protection and encryption indications for the PDU session on MgNB is modified or refreshed, the MgNB shall inform SgNB the new UP integrity protection and encryption indications decision to SgNB in the SgNB Addition/Modification Request message. The SgNB shall update its handling of the UP integrity protection and encryption according to the new decisions received from MgNB. Similarly, if the SgNB is allowed to modify or refresh the UP integrity protection and encryption indications (e.g. UP integrity can no longer be supported due to maximum minimum data rate being exceeded), the SgNB shall also inform MgNB the modification in order to make the two PDU sessions transferred via MgNB and SgNB to have the same the UP security policy. In both cases, the MgNB shall inform the new decision to the UE to in RRC Connection Reconfiguration message to keep the UP security policy on UE and NG-RAN consistent.

NOTE: In case there is a possibility that the UP integrity protection and encryption indication status is changed during the session lifetime, the latest URLLC Radio and System Architecture TR 23.725 [2] needs to be taken into account.

### 6.3.3 Evaluation

For URLLC PDU Sessions, the UP integrity protection and encryption protection indications are the same for the redundant PDU Sessions that carry the same user data is via MgNB and SgNB. This solution fulfils such fundamental security requirement.

This solution provides comprehensive handling procedures in case that the UP integrity protection for one of redundant PDU Sessions is different from the other one which is adopted by the second PDU Session (e.g. UP protection in MgNB is on while SgNB is off or vice versa). The same procedure is also applied for encryption protection.

The solution is applicable for the redundant data transmission of URLLC services based on Dual Connectivity architecture. The solution fulfils the potential security requirements of KI #3.

## 6.4 Solution #4: Security support for N3 tunnel redundancy

### 6.4.1 Introduction

This solution addresses Key Issue#1. If the user data is redundant by means of two duplicated N3 tunnels to fulfil the high-reliability feature, as illustrated in figure 6.4.1-1 below, the NDS/IP framework which is used to secure the network domain interfaces should be reused with the following precautions.



Figure 6.4.1-1: redundant transmission architecture

This data redundancy architecture supports the redundant transmission based on two N3 tunnels between a single NG-RAN node and the UPF. In this architecture, it is assumed that the reliability of NG-RAN node, UPF and CP NFs are high enough to fulfil the reliability requirement of URLLC services served by these NFs. For example, due to the deployment environment of backhaul network, the redundant packets will be transferred between UPF and RAN via two independent N3 tunnels, which are associated with a single PDU Session, over different transport layer path to enhance the reliability of service. To be specific, the NG-RAN node, SMF or UPF provides different routing information in the tunnel information (e.g. different IP addresses or different Network Instances) to ensure the two N3 tunnels can be transferred via disjointed transport layer paths. In addition, these routing information is mapped to disjointed transport layer paths according to network deployment configuration. The RAN node and UPF support packet replication and elimination function as referring to TR 23.725 [2] clause 6.4.

The RAN node and UPF support NDS/IP to ensure the security of the N3 interface. The transport of user data over N3 is integrity, confidentiality and replay-protected.

### 6.4.2 Solution details

If the IPsec tunnel is used to protect all N3 tunnels between NG-RAN and UPF, the current mechanism defined in TS 33.501 [3] clause 9.3 and clause 9.1 shall be reused.

The N3 interface for 5GC and 5G-AN according to NDS/IP is specified in TS 33.210 [6]. Traffic on interfaces carrying control plane signalling can be both integrity and confidentiality protected according to NDS/IP.

IPsec ESP implementation shall be done according to RFC 4303 [8] as profiled by TS 33.210 [6]. For IPsec implementation, tunnel mode is mandatory to support while transport mode is optional.

IKEv2 certificate-based authentication implementation shall be done according to TS 33.310. The certificates shall be supported according to the profile described by TS 33.310 [7]. IKEv2 shall be supported conforming to the IKEv2 profile described in TS 33.310 [7].

In order to protect the traffic on the N3 reference point, it is required to implement IPsec ESP and IKEv2 certificate-based authentication. IPsec is mandatory to implement on the NG-RAN. On the core network side, a SEG may be used to terminate the IPsec tunnel.

### 6.4.3 Evaluation

This solution assumes to reuse NDS/IP mechanism as specified in TS 33.210 [6] to protect the redundant packets which are transferred via two independent N3 tunnels over the N3 interfaces. Due to the deployment environment of backhaul network, the reliability of single N3 tunnel may not be considered sufficiently or reliably to support URLLC services. If there is single N3 tunnel between a single NG-RAN mode and the UPF, NDS/IP is already supposed to be used to protect the N3 interface. Traffic on N3 interface carrying control plane signalling can be both integrity and confidentiality protected with NDS/IP. Similarly, NDS/IP is also used for the two redundant N3 tunnels for the same interface which fulfils the requirements of KI #1.

The solution fulfils the potential security requirement of KI #1.

## 6.5 Solution #5: Security for redundant data transmission

### 6.5.1 Introduction

The solution addresses the Key issues # 1 and #2 in the present document. This solution also addresses Key issue #1: Supporting high reliability by redundant transmission in user plane in TR 23.725 [2] and also complies with the related SA2 conclusions specified in TR 23.725 [2] clause 8.1. Adopting different security protection for the redundant user planes at the UE for two different gNBs will increase the computation complexity, drain battery life and impacts the low latency and reliability requirements of the URLLC services. However, the potential danger of applying separate security protection out weights the convenience of using the same security contexts. For example, if the same security key is used for the two redundant user planes, then having one of the two UP paths compromised implies that both the two redundant user planes' security is compromised. To prevent this situation, it is proposed to use a scheme in which cryptographic separation is achieved while using the same key for both of the two redundant user planes, similar to the security procedures for dual connectivity specified in TS 33.501 [3]. This also results in minimal impact to the URLLC requirement specific changes.

### 6.5.2 Solution details

The solution proposes that both PDU sessions transferring via two user plane paths are using the same key based on the SgNB addition procedure of Dual Connectivity. In this case, the MgNB derives the security key (KUR key) from the KgNB and provides it to the SgNB in the SgNB Addition request message over the Xn-C interface between MgNB and SgNB as specified in TS 33.501 [3]. To generate key streams, the MgNB and the SgNB use different input parameters (for example different bearer ID, PDU session ID) combined with the KUR. This way, the cryptographic separation between the MgNB and the SgNB is achieved. The SgNB derives its own security context using other input parameters such as the PDU session information specific to the redundant user plane path, URLLC identification information and any other required information along with KUR to the KDF to derive the security context for the redundant user plane protection. Other input parameters such as the PDU session information to the redundant user plane data protection will ensure cryptographic separation between the redundant user plane data. After that, the MgNB and the SgNB generate their own RRC and UP keys based on KUR and other parameters different from those used by MgNB (e.g. MgNB can send two sets of random values and data counter values to the UE for the purpose of generating different cipher keys and integrity keys in the MgNB and SgNB respectively) as well as UE side as described in Annex A.8 of TS 33.501 [3] except that the input key is KUR .This mechanism can prevent attackers from identifying the related redundant data stream.

During RRC connection establishment between UE and MgNB the KUR is derived at MgNB, where KgNB, information on URLLC connection and PDU session such as their identifiers can be input to the KDF (Key Derivation Function) to derive the key. Random value and data counter value at MgNB, which are sent from MgNB to UE, can also be input to the KDF. Security is established between UE and MgNB, where integrity and confidentiality protection for uplink data (from UE to MgNB) is configured with security keys for URLLC communication. MgNB sends SgNB addition request for URLLC which includes security key, KUR, information indicating that this request is for URLLC, and security capabilities for integrity protection and ciphering used for the data from UE. The security capabilities are the same as the ones used in MgNB.

When two redundant data is transmitting, it is necessary to make separation between multiple redundant PDU sessions handled between UE and gNB. The KUR key is introduced in this proposal for securing the redundant data transmission. KUR key gets refreshed for different PDCP counts when there is a redundant data transmission.

NOTE: KUR key should be the specific key for the URLLC services based on Dual Connectivity architecture. Particularly, if there are only two redundant data transmission PDU sessions of multiple PDU sessions, the specific key KUR key should be used to identify the URLLC services.



Figure 6.5.2-1: Security context derivation procedure

### 6.5.3 Evaluation

The solution fulfils the cryptographic separation requirement of KI #1. Moreover, the solution fulfils the confidential protection and integrity protection for radio bears of redundant transmission requirement of KI #2.

In the Dual connectivity architecture in TS 33.501 [3], MN terminated bearers are protected using the AS keys derived from KgNB and SN terminated bearers are protected using the AS keys derived from KSN. This means the cryptographic separation for radio bearers serving redundant data transmission is already satisfied by the dual connectivity architecture.

The solution #5 attempts to achieve the same goal by deriving new keys from KUR which is derived from KgNB and PDU session parameters as additional input parameters to KDF. This apparently achieves the cryptographic key separation between MN terminated bearers and SN terminated bearers for the redundant data transmission. However, to address the issue of using the same AS root key at MN and SN (KUR), this solution introduces new random parameters in deriving AS keys both at the MN and SN. This, in effect, mimics the existing key separation scheme between MN and SN in DC at a different level of AS key hierarchy (i.e., algorithm key derivation as opposed to AS root key derivation). Therefore, this additional key handling does not introduce security gain over existing security solution for DC.

This solution introduces a new key KUR that is common for MN and SN. When SN changes, the MN may keep using the same KUR and apply new random parameter to generate a new key stream for the SN. This maintains the cryptographic separation between the two bearers in the redundant data transmission. However, this new key stream derivation needs to be performed in addition to and independent of the existing key derivation in the DC security procedure.

The solution can provide key separation between URLLC PDU sessions and non-URLLC PDU sessions. However, it incurs additional key management and key stream generation at the MN/SN and the UE, while the relative advantage over the existing DC security solution appears to be marginal.

6.6 Solution #6: Dynamic UP security policy control for URLLC service

6.6.1 Introduction

This solution addresses Key Issue #4: Security policy for URLLC service.

According to TS 23.501 [4] and TS 23.502 [5], the SMF shall provide the UP security policy to the NG-RAN during the PDU session establishment procedure.

According to TS 23.503 [10], the PCF will authorize the PCC rule and PDU Session related information for dynamic session management policy control considering the QoS requirement of the application.

6.6.2 Solution details

The User Plane Security Policy should be authorized by PCF considering RAN Capability for UP Security Policy enforcement and QoS requirement from applications. The PCF may further optimized the UP Security Policy, e.g. changing "Required" to "Not Needed" or changing "preferred" to "Not needed" The PCF will send the optimized UP Security Policy to the SMF during SM Policy Association Establishment/ Modification as defined in clauses 4.16.4/4.16.5 of TS 23.502 [5] . The SMF determines a User Plane Security Enforcement information for the user plane of a PDU session based on the authorised UP Security Policy provided by PCF if dynamic PCC is deployed.

In conclusion, the Session Management related policy control will be updated as following:

- Add UP Security Policy information in the PDU Session related policy information.

- PCF need to aware the capability on the speed of integrity protection of the serving RAN node to make PCC decision.

The enforcement of UP Security Policy will be updated as following:

- SMF needs to report the UP Security Policy (received from subscription data) to the PCF.

- SMF determines a User Plane Security Enforcement information based on the authorised UP Security Policy provided by PCF.

NOTE: The scenario that redundant PDU Sessions with the same user data transferred via MgNB and SgNB is based on specific deployment. It is assumed that in this scenario the MgNB and SgNB have the same capability. The PCC decision from the PCF(s) will be the same with the same input.

6.6.3 Evaluation

TBD

## 6.7 Solution #7: Security for redundant data transmission using Dual Connectivity

### 6.7.1 Introduction

This security solution address Key Issue #1: ‘Security for redundant transmission' and Key Issue #2: ‘Support of security for high reliability by redundant data transmission in user plane' in the present document and the security solution for Dual Connectivity (DC) specified in TS 33.501 [3] in 5G Rel-15.

In the recommended SA2 solution #1 in TR 23.725 [2], the UE establishes two PDU Sessions with the network, one PDU Session spans from the UE via MgNB to UPF1 acting as the PDU Session Anchor, and the other PDU Session spans from the UE via SgNB to UPF2 acting as the PDU Session Anchor. Based on these two PDU Sessions, two independent paths are set up. UPF1 and UPF2 connect to the same Data Network (DN), even though the traffic via UPF1 and UPF2 may be routed via different user plane nodes within the DN.



Figure 6.7.1-1: Architecture for redundant User Plane paths for URLLC using Dual Connectivity

For one PDU Session used for redundant data transmission it is explicitly requested by Core Network to MgNB that the user plane goes via the MgNB, and for the other (second) PDU Session used for redundant data transmission it is explicitly requested by Core Network to MgNB that the user plane goes via the SgNB using dual connectivity. The MgNB sets up dual connectivity as defined in TS 37.340 [9] so that the sessions have end to end redundant paths. This implies that all DRB(s) established for the second PDU Session which should go via the SgNB will be offloaded to the SgNB by the MgNB. It is important in this scenario that the same key is not used for the two redundant user planes (for the first and second PDU sessions). Otherwise if the same key is used for the two redundant user planes, then if one path is compromised then the second path is compromised as well. Also, if two different keys are used for the two redundant user planes (for the first and second PDU sessions) then the attacker cannot relate the two data streams.

### 6.7.2 Solution details

This solution is a combination of the following two solutions:

- This solution proposes to re-use the security solution for Dual Connectivity (DC) specified in TS 33.501 [3] in 5G Rel-15, where the Master Node (MN) generates the KSN from the KgNB and a SN Counter, and sends the KSN to the SN over the Xn-C. The SN Counter is used as freshness input into KSN derivations as described in TS 33.501 [3]. The MN sends the value of the SN Counter to the UE over the RRC signalling path when it is required to generate a new KSN. The KSN is used to derive further RRC and UP keys that are used between the UE and SN.

- This solution proposes in addition, that the handling of the UP security policy could potentially be handled.

NOTE: How to handle the UP security policy for URLLC services can refer to the solutions as described in the present document, e.g., solution #1, solution #3, solution #8.

The dual connectivity procedure with activation of encryption/decryption and integrity protection follows the steps outlined in the Figure 6.7.2-1.



Figure 6.7.2-1: Security aspects in SN Addition/Modification procedures (MN initiated)

1) As described in step 1 in clause 6.10.2.1 in TS 33.501 [3] for Dual Connectivity.

2) As described in step 2 in clause 6.10.2.1 in TS 33.501 [3] for Dual Connectivity with the following modifications: the handling of the UP security policy could potentially be handled.

3) As described in step 3 in clause 6.10.2.1 in TS 33.501 [3] for Dual Connectivity with the following modifications: the handling of the UP security policy could potentially be handled.

4. As described in step 4 in clause 6.10.2.1 in TS 33.501 [3] for Dual Connectivity.

5. As described in step 5 in clause 6.10.2.1 in TS 33.501 [3] for Dual Connectivity.

6. As described in step 6 in clause 6.10.2.1 in TS 33.501 [3] for Dual Connectivity.

7. As described in step 7 in clause 6.10.2.1 in TS 33.501 [3] for Dual Connectivity.

### 6.7.3 Evaluation

Solution #7 addresses Key Issue #1 and Key Issue #2.

The solution proposes the use of the security solution for Dual Connectivity as a baseline and additionally the use of similar guidelines for the UP security policy of solution #1.

The solution fulfils all the potential security requirements of KI#1 as (a) it provides a security method to protect the redundant transmissions by re-using the security solutions for dual connectivity, (b) it provides cryptographic separation if radio bearers since it proposes to use different keys for the protection of the two separate redundant PDU sessions and (c) the each path of two redundant paths consists of a PDU session with the same security level compared to a single path. The solution fulfils the potential security requirements for KI#2 as both confidentiality and integrity protection are provided for the two redundant PDU sessions.

The advantage of the solution is that it re-uses the procedures for Dual Connectivity with minimal modifications and as a result it has minimal impact on the UE, MN and SN.

## 6.8 Solution #8: Handling of UP security activation status and selection of SN in Dual Connectivity

### 6.8.1 Introduction

This security solution address Key Issue #3: UP security policy handling for multiple PDU sessions established for redundant data transmission in the present document and the security solution for Dual Connectivity (DC) specified in TS 33.501 [3] in 5G Rel-15.

In the recommended SA2 solution #1 in TR 23.725 [2], for one PDU Session it is explicitly requested by Core Network to Master Node (MN) that the user plane path goes via the MN, and for the other (second) PDU Session it is explicitly requested by Core Network to MN that the user plane path goes via the SN using dual connectivity.

The assumption is that the MN and the SN could be either a gNB or an ng-eNB.

There are some potential issues with using this solution for URLLC services:

**Issue 1:**

If the indication for either UP integrity protection or UP encryption or both in the UP security policy enforcement information sent from SMF to the MN, **is set to the value** "**preferred**", then one of the nodes (MN or SN) may choose a different security activation status compared to the other node. The result would be that the DRB's established for the first PDU session and the second PDU session will use different security activation status (for example: UP integrity protection could be activated for one PDU session but not for the second PDU session).

**Issue 2:**

In the case the UP security policy enforcement information sent from SMF to the MN, does not allow the value "preferred" as described in Solution #1 "Security solution for handling UP security policy for multiple PDU sessions for redundant data transmission", the MN may not know in advance if the selected SN can comply to the UP security policy enforcement information sent from the MN to the SN, when offloading the DRB's for the second PDU session to the SN. If the SN cannot comply, then the SN would reject the request from the MN to offload DRB(s) to the SN. In this case the MN may have already established and activated the DRB's with the UE for the first PDU session.

### 6.8.2 Solution details

This solution proposes to re-use the security solution for Dual Connectivity (DC) as specified in TS 33.501 [3] in 5G Rel-15, with the following enhancements for redundant data transmission:

To resolve issue 1 in clause 6.8.1:

- The MN shall store the applied UP security activation status used for the DRB's established for the first PDU session between the MN and the UE. This is to avoid that one of the nodes (MN or SN) chooses a different UP security activation status compared to the other node, for the first and second PDU sessions. The MN shall ensure that the DRB's established between the MN and the UE for the second PDU uses the same UP security activation status as for the DRB's established for the first PDU. The MN shall provide the same stored UP security activation status applied for the first PDU session to the SN, when offloading the DRB's for the second PDU session. The SN shall use the received UP security activation status received from the MN. This would ensure that the same UP security activation status is applied to all the DRB's established for the first and second PDU session.



Figure 6.8.2-1: Applied UP security activation status for two PDU sessions used for redundant data transmission using DC

1. The UE initiates a PDU establishment procedure with the network for a first PDU session.

2. The MgNB stores the UP security activation status used for DRB's established between the MgNB and the UE for the first PDU.

3. The UE initiates a PDU establishment procedure with the network for a second PDU session.

4. The MgNB ensures that the DRB's established between the MgNB and the UE for the second PDU uses the same UP security activation status as used for DRB's established for the first PDU with the same UE.

5. The MgNB establish Dual Connectivity in RAN. The MgNB sends SN Addition/Modification Request to the SgNB including the stored UP security activation status. The SgNB determines whether it can comply with the received UP security activation status for the DRB's established with the UE. The SgNB sends SN Addition/Modification Acknowledge to the MgNB indicating the UP integrity protection and encryption indications to the MgNB. The MgNB sends the RRC Connection Reconfiguration Request to the UE instructing it to configure the new DRBs and/or SRB for the SgNB.

To resolve issue 2 in clause 6.8.1:

- The MN shall be preconfigured or have access with/to information of the supported security in the available SN(s) (for example: whether UP integrity protection is supported in the SN or not). The MN shall take this information into account when selecting the SN. In case UP integrity is supported, then such configuration information is not needed.

### 6.8.3 Evaluation

The proposed solution address key issue #3: UP security policy handling for multiple PDU sessions established for redundant data transmission in the present document and the security solution for Dual Connectivity (DC) specified in TS 33.501 [3].

For solution resolving Issue #1: If the indication for either UP integrity protection or UP encryption or both in the UP security policy enforcement information sent from SMF to the MN, is set to the value "preferred", then this solution ensures that the two redundant paths have the same UP security policy setting.

For solution resolving Issue #2: In the case the UP security policy enforcement information sent from SMF to the MN, does not allow the value "preferred" as described in Solution #1 "Security solution for handling UP security policy for multiple PDU sessions for redundant data transmission", this solution ensures that the MN knows in advance, even before it has established and activated the DRB's with the UE for the first PDU session, whether the selected SN can comply to the UP security policy enforcement information sent from the MN to the SN, when offloading the DRB's for the second PDU session to the SN. For example if UP integrity protection is "required" but SN does not support UP integrity protection.

Based on above analysis of the proposed solutions for resolving Issue #1 and Issue#2, this solution is able to meet the potential security requirements of KI #3.

# 7 Conclusions

Summary for Key issues and corresponding solutions

The key issues and the corresponding solutions in the present document are listed in the following table.

Table 7.1

| Key issue | | Potential security requirements | Potential Solutions |
| --- | --- | --- | --- |
| #1 | Security for redundant transmission | 1) The 5G system shall provide an appropriate security method to protect the redundant transmission.  2) The system shall provide cryptographic separation for radio bearers serving redundant transmissions.  3) The added paths for redundancy shall provide equal level of security compared to single path. | Solution #4: Security support for N3 tunnel redundancy  Solution #5: Security for redundant data transmission  Solution #7: Security for redundant data transmission using Dual Connectivity |
| #2 | Support of security for high reliability by redundant data transmission in user plane | 1) Confidentiality protection over the air shall be supported for UP data via redundant multiple transmission paths.  2) Integrity protection over the air shall be supported for UP data via redundant multiple transmission paths. | Solution #5: Security for redundant data transmission  Solution #7: Security for redundant data transmission using Dual Connectivity |
| #3 | UP security policy handling for multiple PDU sessions established for redundant data transmission | 1) If encryption of user plane data is enabled between the UE and the gNB on the first path for a first PDU session, then encryption shall be enabled for redundant user data transmission over a second path for a second PDU session as well.  2) If integrity protection of user plane data is enabled between the UE and the gNB on the first path for a first PDU session, then integrity protection shall be enabled for redundant user data transmission over a second path for a second PDU session as well.  3) When Dual Connectivity is used, the MgNB shall ensure that the UP security policy assigned to the MgNB is forwarded and used by the SgNB for the two PDU Sessions used for redundant data transmission. | Solution #1: Security solution for handling UP security policy for multiple PDU sessions for redundant data transmission.  Solution #3: Security policy handling for redundant transmission  Solution #8: Handling of UP security activation status and selection of SN in Dual Connectivity |
| #4 | Security policy for URLLC service | 1) The 5G system shall provide a user plane security policy mechanism applicable to URLLC services.  2) The 5G system shall provide the mechanism for how to enforce User Plane Security Policy when there are URLLC services in the PDU Session.  3）The selection of the security policy shall be under network control. | Solution #3: Security policy handling for redundant transmission  Solution #6: Dynamic UP security policy control for URLLC service |
| #5 | Security aspect of low latency handover procedure | The 5G system shall provide the proper security protection for the optimized URLLC handover procedure. | No solution is available yet in the present document. |
| #6 | Retaining AS security keys for redundant data transmission in user plane | No potential security requirement is recommended. | Solution #2: Retaining AS security keys for redundant data transmission in user plane. |
| #7 | QoS monitoring protection | The 5G system shall be able to protect the 5G E2E QoS Enforcement procedure for a service. | No solution is available yet in the present document. |
| #8 | Acceleration of authentication and key agreement procedure for low latency | No potential security requirement is recommended. | No solution is available yet in the present document. |
| #9 | Security aspect of low latency Re-authentication procedure | No potential security requirement is recommended. | No solution is available yet in the present document. |
| #10 | UP security performance for low latency | No potential security requirement is recommended. | No solution is available yet in the present document. |

## 7.1 Key Issue #1: Security for redundant transmission

For Key Issue #1, it is recommended that the normative work proceed as follows:

- Solution #4 is used as the baseline for ensuring that the security protection in case the redundant traffic is fulfilled by independent N3 tunnels.

- Solution #7 is used as the baseline to ensure security and cryptographic separation for the different radio bearers serving redundant transmissions based on Dual Connectivity architecture. It is agreed that the different UP integrity keys and UP encryption keys are used for the radio bearers serving those redundant transmissions.

## 7.2 Key Issue #2: Support of security for high reliability by redundant data transmission in user plane

For Key Issue #2, it is recommended that solution #7 is taken into account as the basis for normative work.

## 7.3 Key Issue #3: UP security policy handling for multiple PDU sessions established for redundant data transmission

For Key Issue #3, it is recommended that the solution #8 is used as the basis for the normative work to address the issue of UP security policy handling for multiple PDU sessions established for redundant data transmission.

## 7.4 Key Issue #4: Security policy for URLLC service

For Key Issue #4, the normative work shall proceed as follows:

- Solution #1 is used as the basis for normative work to address how to modify the User Plane Security Policy to be specific for URLLC service.

- It is recommended to take the solution #8 as the basis to address the user plane security policy aspect of URLLC. (See also the conclusion of Key Issue #3.)

## 7.6 Key Issue #6: Retaining AS security keys for redundant data transmission in user plane

For Key Issue #6, it is recommended that solution #2 is used as the basis for normative work to address how to retain the AS security keys for URLLC services during the intra-gNB-CU (if the gNB is split into CU and DU) or intra-gNB handover.

## 7.8 Key Issue #8: Acceleration of authentication and key agreement procedure for low latency

Authentication and key agreement is essential for network access and shall not be sacrificed to support low latency communication. The AKA delay is only incurred during the very initial registration, while user plane key refresh is quickly performed (e.g., based on the intra-cell handover procedure). Furthermore, URLLC is for user plane traffic according to TR 23.725 [2], hence AKA procedure is irrelevant. Therefore, it is concluded that any AKA optimization is not pursued for URLLC services.

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2019-09 | SA#85 | SP-190699 |  |  |  | Presented for approval | 2.0.0 |
| 2019-09 | SA#85 | SP-190896 |  |  |  | Revised to introduced the right version of the draft | 2.0.1 |
| 2019-09 | SA#85 |  |  |  |  | Change control version | 16.0.0 |
| 2019-10 |  |  |  |  |  | EditHelp review | 16.0.1 |