



# Rel-19 View - Services & System Aspects

Yusuke Nakano  
KDDI Corporation



# Outline

 From both aspects;

- 1) the gap identified between existing 5G specifications and operators' assumption for commercial implementation
- 2) further enhancement of 5G-Advanced system to meet industrial requirements in future

KDDI prefers to discuss topics in Rel-19 as follows;

- Multi-access PDU session enhancement
- Network initiated slice selection
- Enabling a cryptographic algorithm transition to 256-bits



# Overall View on Rel-19 Content

S.NO.	Title	Brief Description and Key Objectives	Related Stage-1 Study/Work Item	Lead Stage-2 WG	RAN dependencies	Other WG dependencies
1	<b>MA-PDU session enhancement</b>  (See slide 10-14 and SWS-230049 for more details)	This study aims to address restrictions of multiple connectivity features in existing specifications through work tasks as follows;  <b>Key Work Tasks includes defining -</b> <ol style="list-style-type: none"> <li>To study service impact to support MA PDU session with "NR/5GC and NR/5GC" combination.</li> <li>To study service impact to support MA PDU session with "NR/5GC and LTE/EPC" combination</li> </ol>	Yes, FS_DualSteer, TR 22.841	SA2	Don't know.	SA3 for security, SA5 for charging
2.	<b>Network initiated slice selection</b>  (See slide 15-17 and SWS-230044 for more details)	This proposal aims to study procedures for NW initiated slice selection should be studied in addition to existing slice selection solution which assumes the use of URSP;  <b>Key Work Tasks includes defining -</b> <ol style="list-style-type: none"> <li>How to enable selection of a network slice based on the notification from the network side</li> <li>How to enable trusted 3rd party to trigger the notification for the slice selection</li> <li>How to enhance existing PDU session modification procedure to enable switching PDU session between the slices</li> </ol>	No	SA2	No	-



# Overall View on Rel-19 Content

S.NO.	Title	Brief Description and Key Objectives	Related Stage-1 Study/Work Item	Lead Stage-2 WG	RAN dependencies	Other WG dependencies
3.	<p><b>Cryptographic algorithm transition to 256-bits</b></p> <p>(See slide 18-21 and SWS-230043 for more details)</p>	<p>This study aims to address open questions and practical challenges related to the transition of symmetric cryptographic algorithms in the 3GPP System to 256-bit;</p> <p><b>Key Work Tasks includes defining -</b></p> <ol style="list-style-type: none"> <li>1. Study key issues and candidate solutions concerning the negotiation of key sizes between UE and network</li> <li>2. Study key issues and candidate solutions concerning the negotiation of MAC lengths between UE and network</li> <li>3. Study key issues and candidate solutions concerning varying levels of support for 256-bit algorithms in the UE and network</li> </ol>	No	SA3	Don't know.	None identified yet.



# Content1: MA-PDU session enhancement

-  This study aims to address restrictions of multiple connectivity features in existing specifications through work tasks as follows;
- To study service impact to support MA PDU session with "NR/5GC and NR/5GC" combination
  - To study service impact to support MA PDU session with "NR/5GC and LTE/EPC" combination



## Content2: Network initiated slice selection

-  This proposal aims to study procedures for NW initiated slice selection should be studied in addition to existing slice selection solution which assumes the use of URSP;
- how to enable selection of a network slice based on the notification from the network side
  - how to enable trusted 3rd party to trigger the notification for the slice selection
  - how to enhance existing PDU session modification procedure to enable switching PDU session between the slices



## Content3: Cryptographic algorithm transition to 256-bits

-  This study aims to address open questions and practical challenges related to the transition of symmetric cryptographic algorithms in the 3GPP System to 256-bit:
- Study key issues and candidate solutions concerning the negotiation of key sizes between UE and network
  - Study key issues and candidate solutions concerning the negotiation of MAC lengths between UE and network
  - Study key issues and candidate solutions concerning varying levels of support for 256-bit algorithms in the UE and network



Thank you!



# Backup slides

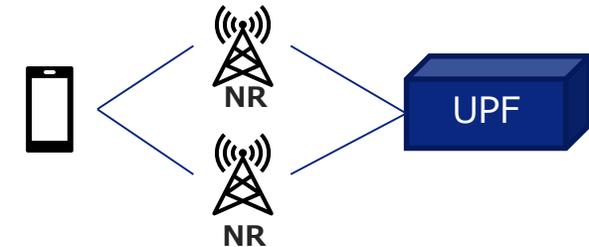


# 1. MA-PDU session enhancement

# Overview

## Motivation

- The proposal is to support MA PDU Session with "NR/5GC and NR/5GC" combination. Both NR RANs belong to the same PLMN.

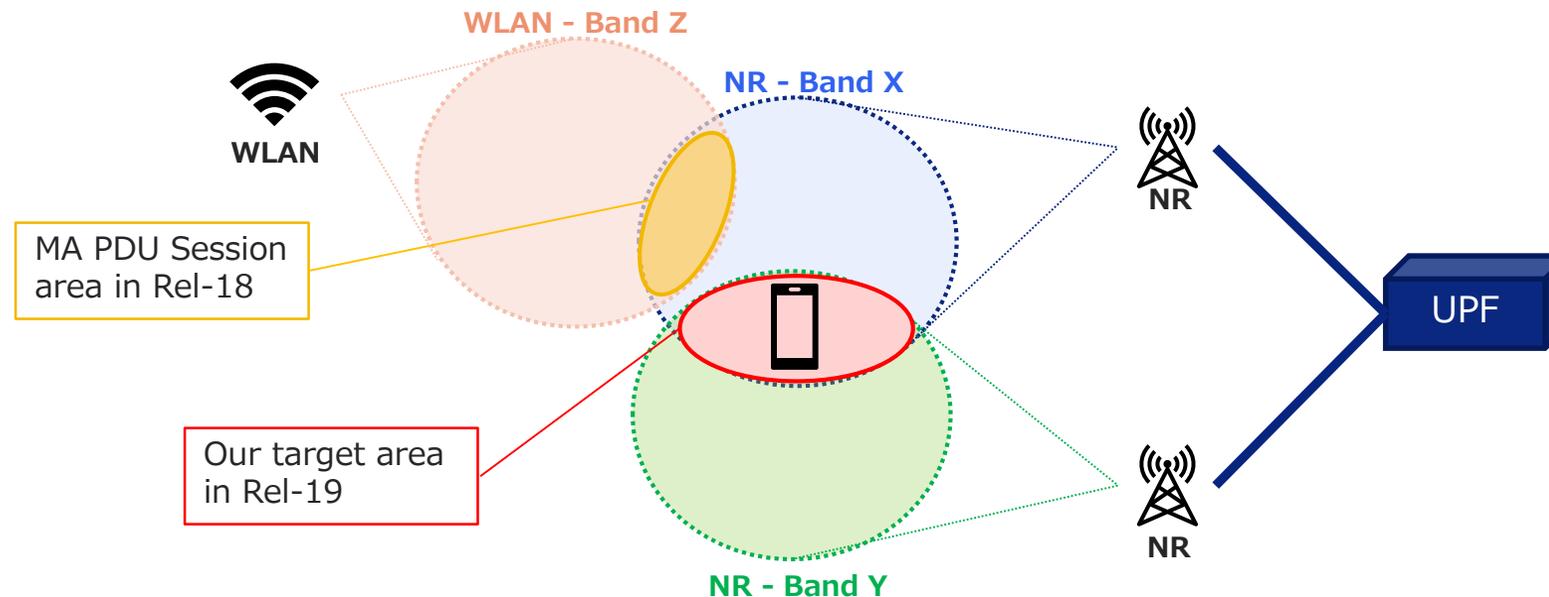


- Utilize MA-PDU session for high-data-rate communication, not only for redundancy
- Example use case: XR communication
- Relevant requirements is in SA1 Rel-19 FS\_DualSteer, TR 22.841

# Restrictions in previous releases

In Rel-18, ATSSS is limited to one 3GPP access and one non-3GPP access combination

- Therefore, it cannot be used in the areas without non-3gpp access

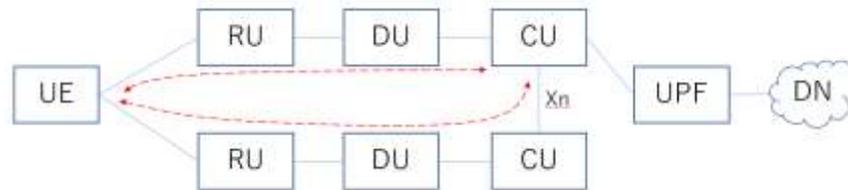


In this case, “Dual Connectivity” can be used for higher capacity, but DC may not be sufficient

# Restrictions in previous releases

- “Dual Connectivity” is a technology that uses two NR paths to increase capacity
- There are two patterns of DC's U-Plane architecture, and both may not be sufficient for higher capacity requirement

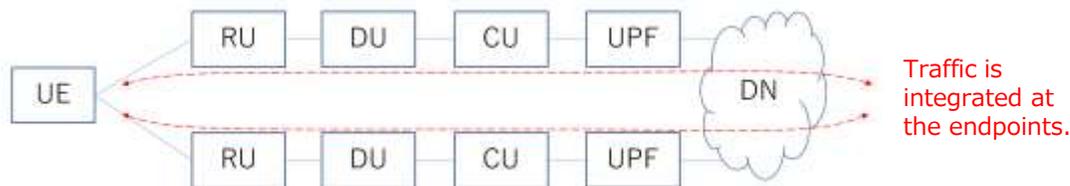
1. Split and integrate transmission data at the PDCP layer of UE/CU



Gaps:

- Xn interface can be a bottleneck.
- Since the data must be integrated at the CU, the delay value of the larger-delay path is applied.

2. DC for E2E redundant communication



Gaps:

- This pattern is only for redundant transmission and cannot be used for higher-data-rate communication.

- The gaps can be filled by “MA PDU Session with NR and NR”



# Proposal

## Objective

- Study service impact to support MA PDU Session with "NR/5GC and NR/5GC" combination
  - e.g., Registration, PDU Session Establishment/Modification, Handover, etc

 This topic can be studied in DualSteer in SA2



## 2. NW initiated slice selection



# Outline

## Definition

Procedures for NW initiated slice selection should be studied in addition to existing slice selection solution which assumes the use of URSP.

## Justification

Existing 3GPP system allows: 1) a UE can select a network slice based on the URSP rule; 2) a 3rd party can provide input for URSP determination to 5GS via NEF “Application guidance for URSP determination” API; 3) PDU session modification with Alternative S-NSSAI triggered by the specific slice condition i.e., service unavailability or congestion. All these features assume the usage of URSP for the network slice selection. This situation causes a restriction for operators to provide optimal network connection through the network slice.

## Usage scenario

The user can enjoy the application on their device via the network connection which is optimally tailored using the network slice. Based on the user’s choice of application, the application client and server work together to request the 3GPP system to provide the optimal network connection.

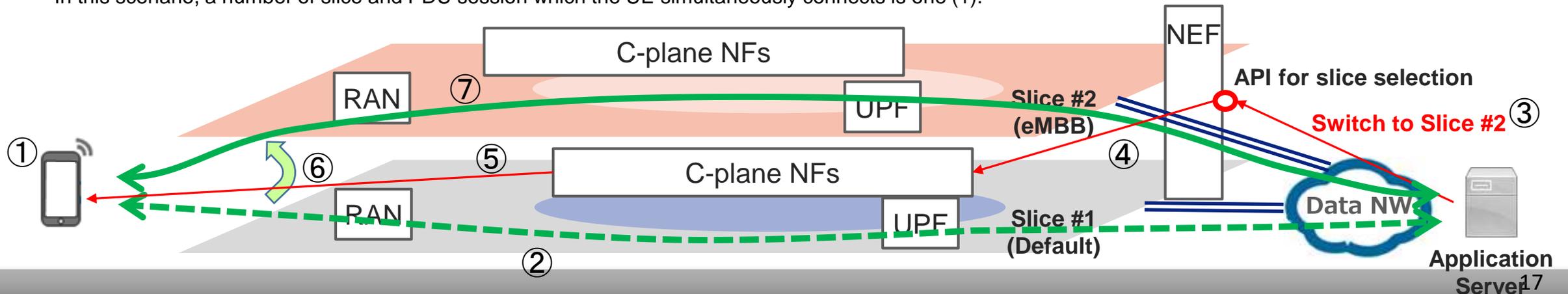


# Possible scenario – Flow assumption

- ① The user activates the application on the UE. The user subscribes a bundle service provided by the operator. The application under the bundle service is allowed to use the special slice (i.e., slice #2 in this scenario).  
NOTE: In this example, the application requires high speed connection.
- ② The application negotiates with the application server via the default slice.
- ③ The application server requests to switch the specific session from the default slice to the other slice (eMBB slice in this example) via NEF, based on the bundle service agreement with the operator.
- ④ NEF requests 5GC to switch the session.
- NOTE: The detail of the procedure (e.g., which NF triggers the procedure) to be studied.
- ⑤ 5GC executes a PDU session modification procedure.
- ⑥ A PDU session is established on the other slice (in this example, slice#2).
- ⑦ UL/DL data is transferred via the PDU session.

## Preconditions;

- The UE has subscribed both slices.
- The application provider and the operator have agreed to provide the bundle service.
- In this scenario, a number of slice and PDU session which the UE simultaneously connects is one (1).





# 3. Cryptographic algorithm transition to 256-bits



# Background

- 📶 3GPP SA3 has previously performed a study on the support of 256-bit algorithms for 5G in TR 33.841 (Rel.16, March 2019)
  - Conclusion: *`... it is proposed for evaluation of new algorithms [by ETSI SAGE] to start now`*
- 📶 ETSI SAGE finalized their evaluation on AES-256, SNOW-V, ZUC-256 ([S3-230642](#))
- 📶 Final version of TR 33.841 contains a number of unresolved Editor's notes
- 📶 SA3 has been discussing the transition to 256-bit algorithms
  - WID proposal presented at SA3#110: Introduction of 256-bit algorithms ([S3-230695](#))
  - Earlier version of this SID, presented at SA3#110 ([S3-230834](#))
  - Offline call on 256-bits was held May 9<sup>th</sup> (Refer to Appendix)

Note: The WID aims to create the required TSs and CRs to TS 33.501 to adopt 256-bit algorithm variants. The SID aims to resolve practical challenges related to the transition to those algorithms.



# Justification

- 🌿 TR 33.841 leaves a number of important questions unanswered and practical challenges not covered associated with the transition to 256-bit algorithms
- 🌿 KDDI foresees challenges that require further study, including but not limited to:
  - Security risks associated to parallel support for 128 and 256-bit algorithms
    1. Risk of inconsistent key sizes being used at different points of the network
    2. Similar risk identified in 5G NSA deployment scenarios
    3. Ensuring sufficient entropy in long-term keys for 256-bit AS/NAS security algorithms
  - Other open questions
    1. Negotiation of MAC lengths between the UE and network as well as system and performance impacts associated with use of MAC tags longer than 32 bits
    2. Negotiation of key lengths between the UE and network as well as expected ABBA parameter values in context of transition



# Objectives

-  This study aims to address open questions and practical challenges related to the transition of symmetric cryptographic algorithms in the 3GPP System to 256-bit:
- Study key issues and candidate solutions concerning the negotiation of key sizes between UE and network incl.:
    - Potential risks supporting 128-bit and 256-bit algorithms in parallel
    - If and how to utilize ABBA parameter
  - Study key issues and candidate solutions concerning the negotiation of MAC lengths between UE and network:
    - System and performance impacts associated with use of longer MACs
    - Secure negotiation of MAC lengths between UE and network
  - Study key issues and candidate solutions concerning varying levels of support for 256-bit algorithms in the UE and network:
    - Ensuring consistent use of 256-bit algorithms
    - Ensuring effective key length equals the key bit length