

# Overview of Preferred SA Release 19 Features

Lenovo



# Outline

## Continue Enhancing 5G Advanced Features

- ATSSS extensions
- Analytics, AI/ML
- XRM
- Sidelink support for TSC

## New Rel 19 Features

- User Identifiers
- Sensing
- Ambient IoT



# Overall View on Rel-19 Content (SA2 topics)

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>ATSSS extensions/ DualSteer</b> (See slide 6)	<ul style="list-style-type: none"> <li>Support DualSteer stage 1 requirements</li> <li>General enhancements from R18</li> </ul>	FS_DualSteer	SA2	None	SA3
2	<b>Analytics &amp; AI/ML</b> (See slide 7)	<ul style="list-style-type: none"> <li>Prescriptive analytics, conflict resolution, coordination between NWDAF, MDAS, ADAES</li> <li>Data collection enhancements</li> <li>AI/ML model distribution enhancements</li> <li>FL multi-domain enhancements</li> </ul>		SA2	Maybe	SA3 for security SA5 MDAS SA6 ADAES
3	<b>Supporting user identities in 3GPP</b> (see slide 8)	<ul style="list-style-type: none"> <li>Supporting third party user identities (digital id, avatars)</li> </ul>	UUI5, FS_Metaverse	SA2		SA3, SA4
4	<b>XRM enhancements</b> (See slide 9)	<ul style="list-style-type: none"> <li>Support XRM via non-3GPP access</li> <li>PDU-set handling enhancements</li> <li>Charging enhancements</li> <li>Analytics enhancements</li> </ul>		SA2	Yes	SA4, SA5 for charging



# Overall View on Rel-19 Content (SA2 topics)

S.NO.	Title	Brief Description and Key Objectives	Related Stage-1 Study/Work Item	Lead Stage-2 WG	RAN dependencies	Other WG dependencies
5	<b>5GC support for Sensing</b> (see slide 10)	<ul style="list-style-type: none"> <li>Define network architecture framework</li> <li>Procedures to support Sensing</li> <li>Non-3GPP sensing</li> </ul>	FS_Sensing	SA2	Depends on SA2 scope	SA6, SA3
6	<b>Ambient IoT</b> (see slide 11)	<ul style="list-style-type: none"> <li>Ambient IoT device identification</li> <li>Registration and connectivity management</li> <li>Support of direct and indirect type of communication</li> </ul>	FS_AmbientIoT	SA2	Yes	SA3
7	<b>Sidelink support for TSC communication</b> (see slide 12)	<ul style="list-style-type: none"> <li>Support stage 1 requirements for:                             <ul style="list-style-type: none"> <li>Clock synchronization to a group of UEs via ProSe direct/indirect communication</li> <li>Support TSC communication via ProSe direct/indirect communication</li> </ul> </li> <li>Support Prose Direct/Indirect communication in private networks (SNPN, PNI-NPN)</li> </ul>	eCAV, TS 22.104	SA2	Yes (URLLC aspects)	No



# Overall View on Rel-19 Content (SA3 topics)

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>Zero Trust Security</b> (slide 13)	<ul style="list-style-type: none"> <li>How to enable security evaluation and minimizing impacts if a security breach occurs (e.g., if a NF is compromised and behaves maliciously)</li> <li>What data need to be collected related to NF and provided to a function (i.e., external to 3GPP domain) to enable security evaluation &amp; monitoring. The external function is up to the operator implementation and outside the scope of 3GPP domain.</li> <li>How to adapt Zero Trust approach to prevent the threat lateral movement and further compromises limiting the threats and associated risks.</li> </ul>	Not Applicable	SA3	None	None
2	<b>Security Optimizations for QUIC</b> (slide 14)	<ul style="list-style-type: none"> <li>Objective is to avoid the “double-layer” protection and make transport of traffic via MP-QUIC more efficient.</li> </ul>	Not Applicable	SA3	none	SA2 maybe
3	<b>Security Enhancements for URSP in Roaming Scenarios</b> (slide 15)	<ul style="list-style-type: none"> <li>Whether there is sensitive information in the URSP rules that can be misused in the serving network</li> <li>How to protect the sensitive information, if any, in the URSP rules towards the UE</li> </ul>	Not Applicable	SA3	none	SA2 maybe



# ATSSS Extensions including support for Dual Steer (ATSSS-DS)

## 🌿 Objectives to support DualSteer requirements:

- Address only scenarios where the UE has a single subscription.
- MA PDU Session shall be able to have two 3GPP access paths (plus a non-3GPP access path) in the same PLMN.
- MA PDU Session shall be able to have two 3GPP access paths (plus a non-3GPP access path) across different PLMNs (e.g., HPLMN + VPLMN, VPLMN + VPLMN, HPLMN + SNPN, VPLMN + SNPN).
- UE shall be able to simultaneously connect to two different VPLMNs.
- UE shall be able to register to 5GC via two 3GPP accesses (plus non-3GPP accesses) via the same or different PLMNs.
- Access path switching shall be supported for several scenarios:
  - Intra-PLMN scenarios: A 3GPP access path shall be switched to another 3GPP access path (or to a non-3GPP access path) in the same PLMN.
  - Inter-PLMN scenarios: A 3GPP access path shall be switched to another 3GPP access path (or to a non-3GPP access path) in a different PLMN.
  - Switching a 3GPP access path to a non-3GPP access path shall be supported (and vice versa).

## 🌿 Objectives for additional enhancements:

- Study how to support steering, switching, and splitting of non-IP traffic (e.g., Ethernet).
- Support an MA PDU Session using a Branching Point (IPv6 multi-homing) or an UL Classifier.
- Support the establishment of an MA PDU Session to a LADN.

# Analytics & AI/ML

## Analytics recommendations/prescriptive analytics:

- Analytics architecture framework enhancements to avoid conflicting actions between different NF types.
- Better coordination between NWDAF, MDAS and ADAES.

## Data Collection Enhancements

- Data Preparation: Analyze and prepare data for use by specific AI/ML model. Each Analytics ID and ML model may need a different data preparation and shall be able to select.
  - Data analysis to derive data characteristics and identify irregularities.
  - Data recovery and cleaning, data formatting (incl. labelling) and prepare data sets.

## AI/ML model distribution enhancements

- AI/ML Model sharing: Introduce Transfer Learning by defining ML model profile to describe model inference and training capabilities.

## FL enhancements

- Support FL amongst different domains (RAN, Core, OAM).
- FL in roaming scenarios (UEs participating in FL are connected to different PLMNs).



# Supporting user identities in 3GPP

## A user may have use of multiple “user identities” to authenticate/access 3rd party services

- A user identity can be a “digital representation” which can include digital identity or avatar identity.

## Study focus

- Creation of a user identity profile in the 3GPP network associated with a 3GPP subscription.
- Identifying tailored service experience in the 3GPP network for a user (e.g. when a user is identified using a user identity when requesting a data connection in the 3GPP network).

# XRM enhancements

## Enhanced PDU set handling

- Inter-PDU set dependency (leftover from R18).
  - There is no information at the NG-RAN to be aware of the dependency of a PDU-set to other PDU-set(s). UE needs reception of PDUs of a PDU-set to decode PDUs of other PDU sets (e.g. reception of P-frames following an I-frame).
- PDU set importance for unmarked PDUs.
  - Currently a default PDU set importance is configured at UPF. Potential enhancements for AF providing PDU-set importance of one or more streams within an AF session (e.g. video, audio and RTCP frames).

## Enhancements on traffic detection and QoS flow mapping for mixed data flows

- e.g., audio, video, haptic streams, multiplexed in a single media flow.

## Differentiated charging for XRM traffic (SA5)

- Charging rate may be different for data with PDU set handling and without PDU set handling.

## Support XRM via non-3GPP access

- PDU set transmission via non-3GPP.
- PDU set QoS control via non-3GPP.

## Study analytics enhancements in order to optimise XRM services

- E.g. Leverage NWDAF analytics to determine optimal PDU-set handling parameters.

# 5GC support for Sensing

## Network architecture enhancement for Sensing

- SA2 to define the core architecture to support sensing using either 3GPP or non-3GPP sensing nodes.

## Identify procedures to support Sensing

- Sensing entities registration and management.
- Sensing service request, authorization.
- Sensing node discovery, selection, configuration.
- 3GPP/non-3GPP sensing data collection and handling.
- Exposure of sensing service capabilities, sensing results.
- Sensing service continuity.
- QoS model and policy enhancement.
- Secure sensing data generation and handling (SA3 impact).

# Ambient IoT

## Ambient IoT device (or service) identification

- Types of devices and device capabilities (e.g. whether to support type A, B, C).
- Device (or group of devices or A-IoT service) identifier and subscription management.

## Registration and connectivity management

- Whether device (or group of devices, or A-IoT service) registration in the 5GS is needed.
  - Authentication and authorization (also SA3 relevant).
- Connection Management for an Ambient IoT device, e.g. CM states, whether paging is supported, etc.
- Ambient IoT Communication service:
  - Define signalling procedures and data transfer (e.g. CP vs. UP data transfer).
  - Network exposure capability for third party Afs.

## Support of direct or indirect type of communication



# Sidelink support for TSC communication

➤ **The following Stage 1 requirements described in 3GPP TS 22.104 for supporting direct device communication are of importance in stage 2 (further details in Clause 7 of 22.104).**

- Support direct device connection between a group of UEs for periodic deterministic communication (both unicast and multicast) with respective service performance requirements in Table 5.2-1 related to cooperative carrying.
- Support clock synchronization (working clock domain) between the UEs within the group of UEs using ProSe direct device communication.
- Similar requirements are also specified for ProSe indirect communication (clause 8, 3GPP TS 22.104).

➤ **Main focus of the study:**

- Based on stage 1 requirements identify enhancements needed in scenarios where 5GS is deployed as a layer-2 ethernet bridge when integrated with IEEE TSN network in order to support:
  - Clock synchronization of a common working clock between a group of UEs using ProSe Direct/Indirect Communication.
  - TSN stream communication via ProSe Direct/Indirect Communication.
- Identify enhancements needed to support of ProSe Direct/Indirect Communication in private networks (SNPN and PNI-NPN).



# Zero Trust Security (ZTS) (SA3)

- **Possible extension of ZTS study from current Rel-18 to Rel-19 (if not completed).**
- **Service Access and Interactions in 5G system is built on certain security principles:**
  - Authentication and/or Authorization.
  - Secured connection establishment.
- **Trust over a NF/AF can't be assumed static and intact throughout its lifetime as a compromised NF can give way for lateral movement of the attack.**
  - If any NF gets compromised can impact UE services or other connected NFs.
- **The objective(s) to study:**
  - How to enable security evaluation and minimizing impacts if a security breach occurs (e.g., if a NF is compromised and behaves maliciously).
    - What data need to be collected related to NF and provided to a function (i.e., external to 3GPP domain) to enable security evaluation & monitoring. The external function is up to the operator implementation and outside the scope of 3GPP domain.
  - How to adapt Zero Trust approach to prevent the threat lateral movement and further compromises limiting the threats and associated risks.



# Security Optimizations for QUIC (SA3)

- ATSSS\_ph3 defined support for Multipath QUIC between the UE and the UPF. MP-QUIC extends QUIC (RFC 9000) to enable simultaneous use of multiple paths between two endpoints (UE and UPF).
- QUIC mandates the usage of TLS 1.3 with encryption according to RFC 8446. Hence, traffic routed via MP-QUIC is protected using QUIC security mechanisms *and* 3GPP UP security mechanisms.
- **Objective is to avoid the “double-layer” protection and make transport of traffic via MP-QUIC more efficient.**



# Security Enhancements for URSP in Roaming Scenarios (SA3)

## In roaming scenarios, URSP rules are sent from HPLMN to UE, via VPLMN, without any security protection

- SA3 never analyzed the possible attacks and frauds that could be carried out in such roaming cases.
- For example, it is possible for VPLMN to change the URSP rules received from HPLMN.

## Objectives of the study

- Whether there is sensitive information in the URSP rules that can be misused in the serving network.
- How to protect the sensitive information, if any, in the URSP rules towards the UE.



# Thanks!