

# 3GPP SA Rel-19 Initial Views

MITRE

# Outline

-  Overall View on Rel-19 Content
-  Content Details
-  Summary: General Considerations for Rel-19



# 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
N/A	<b>SIM-less Authentication for Non-Public Networks (NPN)</b>  (See slide 9,10 for more details)	5GS shall support operator-controlled alternative authentication methods (i.e. alternative to AKA) with different types of credentials for network access for IoT devices in isolated deployment scenarios (e.g. for industrial automation). It shall also support a suitable framework (e.g. EAP) allowing alternative (e.g., to AKA) authentication methods with non-3GPP identities and credentials to be used for UE network access authentication in NPN. <b>Key Work Tasks includes defining –</b> See Content section pages 6,7	Yes	SA3	Yes	SA2, CT1
N/A	<b>End-to-End Self-Securing and Resilient Network Slices</b>  (See slide 7,8 for more details)	5G system support for E2E network slicing (RAN, transport network and core domains) lack the support of self-securing and resilient capabilities for autonomous security and/or a) dynamically updating the E2E network slicing capabilities when the operational environment changes; and b) ensuring service persistence automatically for the cross networks scenario. Capabilities are essential for use cases such as V2X, next generation (NG) public safety, first responders, and critical infrastructure <b>Key Work Tasks includes defining –</b> See Content Section, pages 4,5	Yes	SA2, SA3	Yes	SA3 for security, SA2 for architecting
N/A	<b>Enhancements to ATSSS in Rel. 19</b>	5GS utilizes Access Traffic Steering, Switching, and Splitting (ATSSS) to enable data transmission techniques. Recently, 3GPP SA1 and SA2 have been working on innovative solutions for possible improvement from different perspectives <b>Key Work Tasks includes defining -</b> <ol style="list-style-type: none"> <li>1. MPQUIC</li> <li>2. Use of IPv6 multi-path</li> <li>3. UL (Upper Layer), LL (Lower Layer) steering capabilities</li> </ol>	Yes, TS 22.261	SA2, RAN3	Yes	SA5 for management and orchestration



# 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
N/A	<p><b>NTN Enhancements for Rel-19 and Beyond</b></p> <p>(See slide 5,6 for more details)</p>	<p>Study 5GS requirements of new E2E services in 5G NTN solutions with satellite networking capabilities such as inter-satellite links, satellite to HAPS connectivity, and satellite to ground communications,</p> <p><b>Key Work Tasks includes defining E2E</b></p> <ol style="list-style-type: none"> <li>1. Services requirements related to Pointing, Acquisition, Tracking</li> <li>2. How packets for these services will be forwarded</li> <li>3. Synchronization and time stamping requirements for PNT-enabled services</li> <li>4. Study benefits of OISL (Optical Inter Satellite Links) to deliver 5G and beyond services with stringent security, low latency, and high throughput requirements</li> </ol>	Yes, 22.261, 22.865	SA2	Yes	CT, SA3

# 5G NTN Enhancements for Rel-19 and Beyond: Background

- NTN is defined in 3GPP Rel 16 – 18 as transparent mode satellite access only
- For Rel-19, SA1 is studying to support new services that need satellites capable of store-and-forward, positioning, GNSS independent operation, and regenerative payloads
  - TR 22.865 captures a set of use cases and potential service requirements related to the 5G system with satellite access
  - RAN has also studied in TR 38.811 *Study on New Radio to Support Non-Terrestrial Networks*, and in TR 38.821 *Solutions for NR to support non-Terrestrial Networks* – radio aspects of these new services, particularly regenerative satellite with ISL, and gNB processed payloads

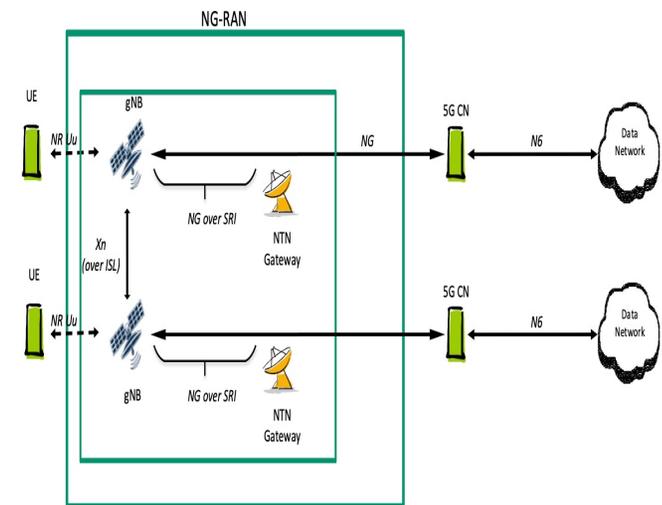


Figure 5.2.1-2: Regenerative satellite with ISL, gNB processed payload

Source: 3GPP TR 38.821  
*Solutions for NR to support non-terrestrial networks (NTN)*

# New 5G Services to Benefit from NTN with Regenerative Payloads, ISL, IAB

- Multiple efforts have demonstrated benefits of satellite networking to provide innovative services (European Space Agency (ESA)-Alphasat, etc.). Mission Critical (MC) services that require fast and reliable communications in remote locations could benefit from further interoperability and/or integration between TN and NTN
- We propose that SA takes on work during Rel 19 looking into 5G services architecture supported by 5G NTN with these topics in focus:
  - For QoS use the existing 5QIs as baseline, and give service providers flexibility to offer diverse services without modifying the baseline but study introducing, for example, scaling factors for KPIs such as error rate and delay
  - Regenerative payloads with ISL/OISL, IAB
- Areas to investigate for these innovative services for Rel-19 and beyond:
  - Requirements related to Pointing, Acquisition, Tracking
  - How packets for these services will be forwarded
  - Requirements of synchronization, time stamping for PNT services
  - OISL transport with stringent latency, spectrum flexibility, cloud computing, and high throughput requirements

# End-to-End Self-Securing and Resilient Network Slices

## Where we are now:

- Pre-provisioned network slicing capabilities
- Capabilities cannot be updated dynamically in near real-time when environment or threat changes
- Network slicing does not support scenario when a user traverses between networks

## Where we want to go:

- Dynamically update end-to-end network slicing capabilities for security and resilience when the operational environment changes (such as spectrum interference and security threats)
- Ensure service persistence between public / private networks as well as between terrestrial networks and non-terrestrial networks (NTNs) scenarios.

# End-to-End Self-Securing and Resilient Network Slices

## ☞ Justification:

- Current 3GPP specifications in E2E network slicing (RAN, transport network and core domains) lack the support of self-securing and resilient capabilities for truly autonomous security. For example, it cannot support a) dynamically updating the E2E network slicing capabilities in security and resilience when the operational environment changes (such as spectrum interference and security threats) and b) ensuring service persistence automatically for the cross networks scenario.
- Capabilities are essential for use cases such as V2X, next generation (NG) public safety, first responders, and critical infrastructure.

## ☞ Problem Statement:

- Network slicing allows the operator to provide customized networks. For example, there can be different requirements on functionality (e.g., security), differences in performance requirements (e.g., availability, reliability).
- The serving 5G network shall support providing connectivity to home and roaming users in the same network slice.
- The 5G system shall provide suitable APIs to coordinate network slices in multiple 5G networks .

## ☞ 5G Areas of Study:

- Enhancements for a E2E network slice to provide high security and resilience in changing operational environments, traversing across elements of a network (intra-network slices), across cells, and networks (inter-network slices) with service persistence providing a better user experience.
- Advanced network data analytics function to perform threat detection, monitoring and statistics/events collection of E2E network slices to evaluate compliance with security and resilience requirements ((re)-configure and (re)-optimize the network slices (e.g., RAN slice and core network slice)) intelligently in near real-time.
- Additional signaling to assess the threat environment by evaluating the statistics, metrics and KPIs collected.
- Signaling to select and enable security and resilience capabilities in different protocol layers, elements, cells and networks for a particular slice based on the assessment results / recommendations.

# SIM-less Authentication for Non-Public Networks (NPN)

## Where we are now:

- Symmetric key-based centralized security architecture. However, almost all other data networking and web services technologies have adopted public key infrastructure (PKI) with digital certificates and asymmetric key systems for security and authentication.

## Where we want to go:

- Distributed authentication architecture where security protection is provided for all messages (broadcast / unicast) even before security context is established
- Adding users to a non-centralized infrastructure network dynamically in a non-public network.

# SIM-less Authentication for Non-Public Networks (NPN)

## Justification:

- The current symmetric key system architecture for authentication cannot support the following scenarios without pre-provisioning.
  - Ad-hoc teaming requirements from multiple entities to effectively accomplish one task (e.g., provide coordinated support in an incident / disaster recovery / humanitarian mission)
  - Adding users (on-the-fly) in infrastructure-less sidelink communications for first responders and V2X. For example: a) Within tunnels or disaster-stricken areas for rescue missions leveraged by multiple first responder teams and b) In advanced V2X use cases where ambulances from different locations form a platoon travelling together to a disaster area and share information about the environment
  - Dynamic network access
- 5G has started using PKI authentication for devices: Subscription Concealed Identifier (SUCI) encryption; Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) based UE authentication and Open Authorization (Oauth) 2.0 framework.

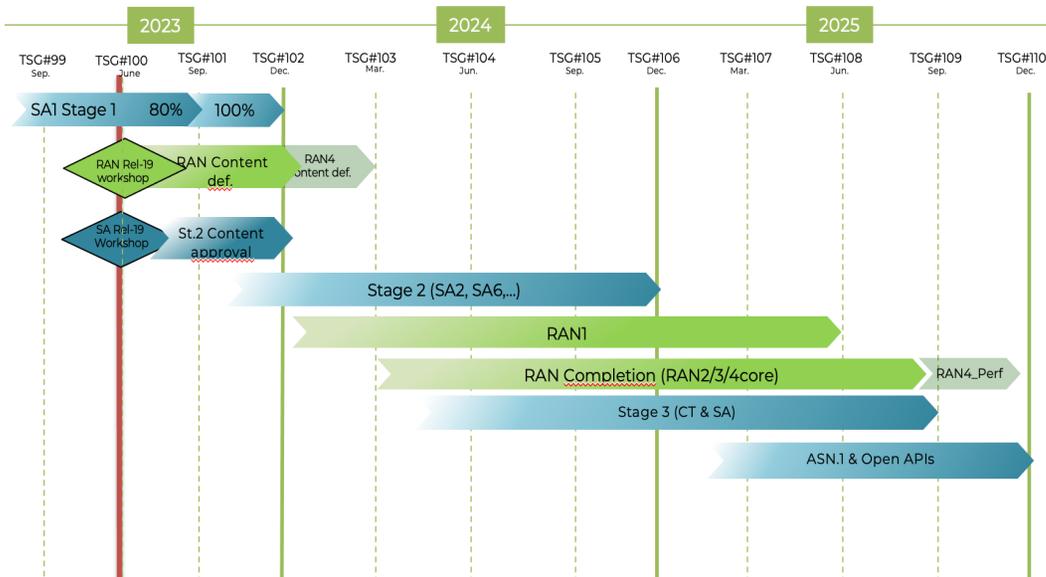
## Problem Statement:

- The 5G system shall support operator-controlled alternative authentication methods (i.e. alternative to AKA) with different types of credentials for network access for IoT devices in isolated deployment scenarios (e.g. for industrial automation).
- The 5G system shall support a suitable framework (e.g. EAP) allowing alternative (e.g., to AKA) authentication methods with non-3GPP identities and credentials to be used for UE network access authentication in non-public networks.

## 5G Areas of Study:

- Feasibility of SIM-less authentication as part of 5G system enhancements. The potential solutions could include:
  - Extension of Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) leveraging PKI / asymmetric key systems for authentication (for example, in infrastructure-less sidelink communication scenarios)
  - Emerging technologies such as blockchain for distributed authentication (e.g., Web3) where the trust model of blockchain adopts a distributed ledger without a centralized infrastructure and is suitable for obtaining a consensus on trust across all nodes in a distributed peer-to-peer network.
- Associated signaling across layers, elements, and networks.

# Summary – General Considerations



Source: SP-230390 Release 19 Schedule Slide

- Support endorsed Rel-19 SA timeline
- Advanced self-securing and resilient 5G
- Rel. 19 is the second release of 5G-Adv call for advanced design principles
  - Cloud, virtualization in SBA
  - AI/ML enablement
  - Edge computing
- Services for traditional operators as well as for new verticals and private networks with innovative QoS, slices, and automation