

**Smarter technology for all**

**Rel.18**

**Discussion for**

**Study on Zero Trust Security**

**(ZTS)**



# Motivation (1/2)

## To Enable Zero Trust Security Adaptations for 5GS

- Service Access and all interactions in 5G system is built on certain Zero Trust security principles such as:
  - Authentication and/or Authorization
  - Secure connection establishment
- Heterogeneity and varied NF deployment options (could be distributed across cloud infrastructure/locations):
  - May run into errors due to configuration issues
  - May get exposure to insider threats
  - May get threats/comprise due to cyber attacks
  - Huge number of connected devices may attempt botnet/DDoS
- Trust over a NF or AF can't be assumed static and intact throughout its lifetime despite all security pre-configurations
- Any NF if gets compromised in its life-time:
  - May impacts set of UEs service
  - May impact other connected NFs (i.e., Lateral movement of the attack)

# Motivation (2/2)

## Zero Trust Security

- The core Zero Trust principle includes:
  - Continuous trust validation and minimizing impacts if any security breach occurs due to external factors (example., end-users) or by an insider (example., compromised or malicious NF)
  - Adaptation of Zero Trust approach in this regard can prevent the threat lateral movement and further compromises limiting the threats and associated risks

Existing 5GS Features assume end-user devices and NFs set with initial access Configurations are implicitly trusted throughout its life-time.

Current system lacks on-demand/real-time trust evaluation.

- Adaptation of Zero Trust principles in 5GS:
  - In advance threat detection, explicit trust evaluation and appropriate handling.
  - Prevents the threat lateral movement and further compromise (limiting the threats & associated risks).
  - Realize full potential benefits for vertical service customers, and business.
  - Ensures service reliability and safety of end users.

# What can we potentially analyse during the course of the study:

*may include but are not limited to:*

- If any NF is compromised, what impacts will it have?
- Do, we have methods to identify the NFs under threat or to identify the one that has been compromised?
- How to evaluate explicit trust specific to any NF involved in the system?
- If we have methods to identify the NF under threat, simply terminating them would impact all the ongoing service.
- Analyse and identify, what more SA3 WG can do to ensure seamless service in this condition while also ensuring security.

# Scope

- **The Objective of the study includes:**

- *Analyse the 3GPP 5GS security scenarios related to the 5G core network that may benefit from a Zero Trust principle and identify the associated threats.*
- *Analyse the suitable Zero Trust security mechanisms (i.e., for enabling trust evaluation and ensuring trust) to address the threats identified where potential security risk exists.*
- *Provide recommendations for a Zero Trust 5GS security architecture, where such recommendations may include 3GPP 5G security requirements, technical enhancements, and procedural enhancements.*

**thanks.**

**Smarter  
technology  
for all**

**Lenovo**