3GPP TSG SA WG3 Meeting #98bis-e *draft-*S3-200723-r1

e-meeting, April 14 - 17 2020

**Agenda item:** 2.5

**Source:** Huawei, Hisilicon

**Title:** Discussion on protection of UE radio capability for CP optimized UEs

**Document for:** Discussion and endorsement

# Introduction

For CIoT devices that only support control-plane optimization, it is necessary to develop a security solution to protect the UE radio capabilities transfer. The ongoing study on CIoT has several related solutions. As SA3 is approaching the planned end-date for this study, this contribution gives a way forward on the solutions.

In this paper, several proposals are listed. Companies may take the observations into considerations and try to get consensus in the e-meeting.

# Discussion

For both EPS and 5G CIoT CP optimized UE, the AS security is not expected to be supported. Without AS security, there are some potential threats for the UE radio capability transfer. The system shall support to mitigate the effects of handling unprotected UE radio capability for UEs without AS security.

**Observation 1: It's needed for both EPS and 5G to protect the UE radio capabilities transfer.**

**Proposal 1: The mechanism, which is applicable and common for both EPS and 5G CIoT UEs, is highly recommended.**

Enabling AS security for CIoT optimization UE can protect the whole connection. But there are several drawbacks as following:

* It requires hardware upgrade, which may unnecessarily increase the cost and complexity;
* It is against architectural decision made by other working groups due to various reasons;
* Involving per-UE AS keys(Note that this parameter cannot be compressed to save spare) in the RAN may require higher storage in RAN, and thus downgrade RAN service capability for CIoT scenarios.
* It’s near the end of R16. The huge impact to other groups should be avoided.

**Observation 2: Enabling AS security for CIoT optimization UE has huge impact.**

The attackers may identify the devices with the reference mode and the acquired capabilities. The potential vulnerabilities applicable to the identified device may be determined. In addition, attackers may cause high battery consumption for CIoT UEs that only support CP optimization due to frequent unauthorized UE radio capability enquiries. The confidentiality-protection for UE radio capability and enquiry messages are needed. A more secure solution is highly recommended.

**Observation 3: The confidentiality-protection for UE radio capability and enquiry message are necessary.**

# Conclusion and Proposal

This paper mainly discusses the issue of protection of radio capabilities, and we have the following proposal:

**Proposal 1: The mechanism, which is applicable and common for both EPS and 5G CIoT UEs, is highly recommended.**