**3GPP TSG SA WG3 (Security) Meeting #105-e S3-213854**

**E-meeting, 08-19 November 2021**

**Source: JSRPC Kryptonite**

**Title: Update to solution #2.4**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

***It is proposed to change the declared security properties of Solution #2.4 in TR 33.846***

# 2 References

[1] 3GPP TR 33.846 V0.13.0, Study on authentication enhancements in 5G System

[2] 3GPP TSG-SA3 Meeting #104-e, [S3-212407](https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionId=1235599)**,** Observations on TR 33.846

# 3 Rationale

As a result of the previous meeting (SA3#104-e) there was published a new document S3-212407 [[2](https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionId=1235599)] containing observations on solutions presented in TR 33.846 [1] and revealing a number of concerns regarding the declared security properties.

The current document contains amendment proposals to the solution from clause 6.2.4 of TR 33.846 [1]. The issue of the need for changes is caused by the attack described in section 2.4 of the S3-212407 [[2](https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionId=1235599)] document, so we invite SA3 to consider these points.

## 3.1 Problem description

According to the TR 33.846 [1] document the solution #2.4 is supposed to address key issue #2.1 (linkability attack by using failure message code, hereinafter referred to as "LFM attack") and key issue #4.1 (protection of SQN during AKA re-synchronisations, hereinafter referred to as "AMA attack").

However, the S3-212407 [[2](https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionId=1235599)] document demonstrates that this solution does not address key issue #2.1 by providing a new variant of LFM attack. The attack consists of three steps (see Figure 1), more details can be found in the S3-212407 [[2](https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionId=1235599)] document:

1. On the first step the adversary intercepts one legitimate authentication request message containing the pair (R, AUTN) sent by the network to UE.
2. On the second step for any victim UE' the adversary replays captured (R, AUTN) and receives the following answer:
	* If UE’ = UE, UE' sends (SYNC\_failure ∥ AUTS ) ⊕ $γ$;
	* If UE’ ≠ UE, UE' sends (MAC\_failure ∥ pseudoAUTS1 ) ⊕ $γ$,

where $γ$ = HMAC-SHA256(KAUSF, R).

1. On the last step the adversary sends to the UE’ captured R and some random pseudoAUTN value. Irrespective of whether UE' = UE the adversary receives the following answer:
	* UE' will send (MAC\_failure ∥ pseudoAUTS2 ) ⊕ $γ$,

where $γ$ is the same as on previous step.

If the masked error code is the same on both steps 2 and 3, then UE’ ≠ UE, otherwise UE’ = UE.

NOTE: The possibility to use the fixed *KEY* (the string of all zeros) to encrypt error codes can potentially lead to security problems if we succeed in forcing UE to use this fixed key (further research is needed to evaluate the possibility of this event).



Figure 1

## 3.2 Proposed changes

Since the solution #2.4 does not address key issue #2.1, we consider it appropriate to make the following change:

* + 1. Add the Editor’s Note to the clause 6.2.4.3 Evaluation.

# 4 Detailed proposals

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 1\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 6.2.4.3 Evaluation

Editor’s Note: This solution does not protect against new variant of LFM attack, which was described in section 2.4 of the [S3-212407](https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionId=1235599). How to address this attack is FFS.

##### 6.2.4.3.1 Active attack

The solution protects against linkability attacks based on recognizing MAC / synchronization failures on the radio interface, and protects the procedure for resynchronization thanks to the addition of new parameter RAND\_Sync.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 1\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*