**3GPP TSG SA WG3 (Security) Meeting #105-e S3-213853**

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

**Source: JSRPC Kryptonite**

**Title: Update to solution #2.3**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

***It is proposed to change the declared security properties of Solution #2.3 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 6.2.3 of TR 33.846 [1]. The issue of the need for changes is caused by the attack described in section 2.3 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 #2.3 is supposed to address key issue #2.1 (linkability attack by using failure message code, hereinafter referred to as "LFM 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 S3-212407 [[2](https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionId=1235599)]:

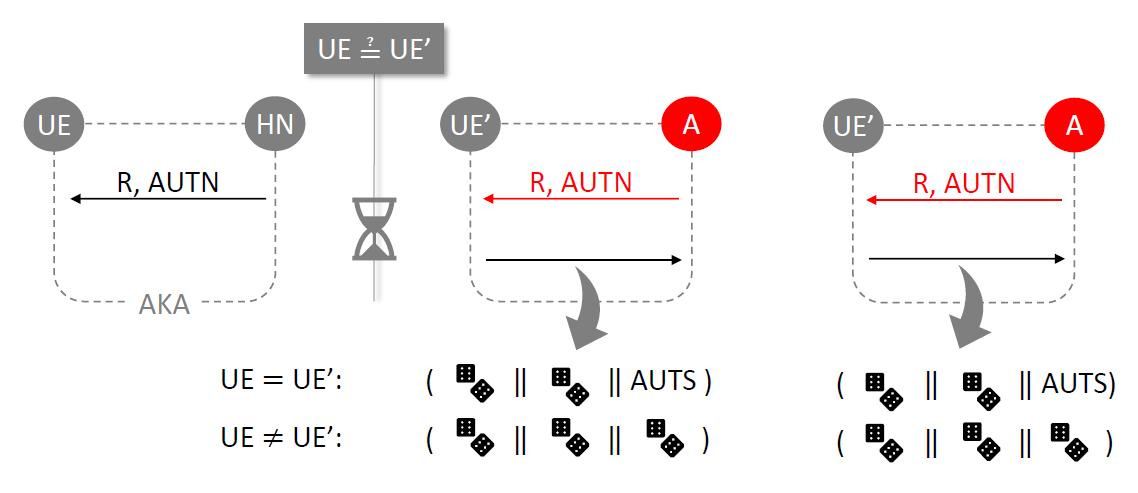


Figure 1

1. On the first step the adversary intercepts one legitimate authentication request message containing the pair (RAND, AUTN) sent by the network to UE.
2. On the second step for any victim UE' the adversary replays captured (RAND, AUTN) and receives the following answer:
   * If UE’ = UE, UE' sends (pseudoRES\*, pseudoCAUSE, AUTS).
   * If UE’ ≠ UE, UE' sends (pseudoRES\*, pseudoCAUSE, pseudoAUTS).
3. On the last step the adversary repeats the step 2.
   * If UE’ = UE, UE' sends (pseudoRES\*, pseudoCAUSE, AUTS). This response contains the same AUTS as in the step 2.
   * If UE’ ≠ UE, UE' sends (pseudoRES\*, pseudoCAUSE, pseudoAUTS). This response contains new freshly generated pseudoAUTS, different from the previously used in the step 2.

If the AUTS value is the same on both steps 2 and 3, then UE’ = UE, otherwise UE’ ≠ UE.

Additionally, we would like to highlight the following points:

* the pseudoCAUSE field is not used;
* if the authentication is correct, then there is no need to send pseudoCAUSE and AUTS, because the adversary can easily distinguish whether the authentication was successful or not using the traffic analysis after the authentication (it is either re-authentication, or further communications).

## 3.2 Proposed changes

Since the solution #2.3 does not address key issue #2.1, we consider it appropriate to make the following changes:

* + 1. Change the description of the Table 6.0-1 fixing the place where the protection against the attack from key issue #2.1 was declared.
    2. Add the NOTE to the clause 6.2.3.3 Evaluation.

# 4 Detailed proposals

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

**Table 6.0-1: Mapping of solutions to key issues**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | **Key Issues** | | | | | | | |
| **Solutions** | | #1.X | #2.1 | | #2.2 | #3.1  \*) | #3.2 | #4.1 |  |  |
| **Solutions for anchor keys security** | |  |  | |  |  |  |  |  |  |
| No solution so far | |  |  | |  |  |  |  |  |  |
| **Solutions for resilience against identifier linkability** | |  |  | |  |  |  |  |  |  |
| #2.1: Handling of Sync failure by AUTS encryption | |  | x | |  |  |  | x |  |  |
| #2.2: Encryption of authentication failure message types by UE with new keys derived from K\_AUSF | |  | x | |  |  |  | x |  |  |
| #2.3: Unified authentication response message by UE | |  |  | |  |  |  |  |  |  |
| #2.4: MAC-S based solution | |  | x | |  |  |  | x |  |  |
| … | | | | | | | | | | |

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 2\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 6.2.3.3 Evaluation

This solution enables the network to mitigate one kind of Linkability attacks which are based on recognising the different authentication responses.

When the UE receives the authentication request message, UE generates authentication response with unified format for successful authentication, MAC failure and sync failure. Successful authentication can be distinguished through verification of RES\* in AMF. MAC failure and sync failure can be differentiated through verification of AUTS in UDM. This solution modifies the original authentication response message as described in TS 24.501 [6] with the idea to provide in failure and success case no evidence of the outcome of authentication that an attacker can see at the air interface.

The attackers are unable to get the failure type with the authentication response message (by not using authentication failure message).

This solution impacts the visited network.

NOTE: This solution does not address Key Issue #2.1, since new variant of LFM attack was described in section 2.3 of the [S3-212407](https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionId=1235599). Futher elaboration is required.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 2\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*