**3GPP TSG-SA3 Meeting #103-e *S3-211518-r1***

**e-meeting, 17 – 28 May 2021** Merge of S3-211518-r1, S3-212111

**Source:** **Nokia, Nokia Shanghai Bell, AT&T**

**Title:** **5G NSWO: EAP-AKA’ authentication for NSWO**

**Document for: Approval**

**Agenda Item: 5.22**

# 1 Decision/action requested

***Approve this contribution to add text in the Key issue#1 for 5G NSWO TR***

# 2 References

[1] SP-210262

# 3 Rationale

The SID for NSWO-5G has been approved in SA#91-e in SP\_210262. The contribution adds a Key Issue in the 5G NSWO TR.

# 4 Detailed proposal

pCR

\*\*\* BEGINNING OF CHANGES (all text new) \*\*\*

# Key issue #X: Support of EAP-AKA’ authentication for NSWO

### 5.X.1 Key issue details

For 5G access authentication, two authentication methods EAP-AKA’ and 5G AKA are supported over both 3GPP access and non-3GPP access. Currently the procedure in 3GPP TS 33.402 which are used for (4G) NSWO over trusted non-3GPP access in 23.402 foresees that the UE may send its IMSI in clear text, i.e. unencrypted, over that air interface and to the AAA server in the core network.To support Non-Seamless Wifi Offload (NSWO) in 5G, authentication mechanisms similar to the primary authentication mechanisms need to be supported. The new NSWO authentication procedures should also in support the same or similar level of security and privacy, i.e. to never expose the IMSI/SUPI in the clear. Since the UEs may be provisioned by the operators to use EAP-AKA, this may be the easiet authentication method to be adopted for 5G NSWO.

Currently installed WLAN APs support only EAP authentication framework over Radius or Diameter interface to an operator owned AAA. Since the 5GC is able to support EAP-AKA’ authentication, that could be extended to support NSWO using the same 3GPP credentials. Since the 5GC is able to support a unified authentication method, including EAP-AKA’ the same could be extended to support NSWO using the same credentials.

Reusing the same EAP-AKA infrastructure for the NSWO authentication can provide 5G equivalent authentication security to enterprise users as well.

### 5.X.2 Security threats

UEs need to be authenticated when they are connected to WLAN APs for availing NSWO, otherwise the NSWO could be misused by fraudulent UEs. Fraudulent UEs accessing enterpise WLAN without authentication can consume the WLAN resources and prevent the NSWO for legitimate UEs. This can cause DDoS scenarios for NSWO UEs.

If subscriber identity privacy is not available during authentication procedure, then tracking of the subscriber with “IMSI catchers” can lead to trackability and linkablity attacks.

### 5.X.3 Potential security requirements

The 5GS shall support EAP-AKA’ authentication method using 5GC credentials for NSWO.

\*\*\* END OF CHANGES \*\*\*