3GPP TSG-SA3 Meeting #117 S3-242xxx

Maastricht, Netherlands 19 - 23 August 2024 (revision of S3-yyxxxx)

**Source:** **Nokia**

**Title: Discussion paper for Fast BSS based NSWO solution**

**Document for: Discussion**

**Agenda Item: 5.10**

# 1 Decision/action requested

***It is requested to discuss the discussion paper on Fast BSS solution issue related to NSWO***

# 2 References

[X]

3 Rationale

Please see details proposal.

# 4 Detailed proposal

For the KI#4 in TR 33.702, few solutions talk about Fast BSS Transition (FT) based solution. In this paper, we try to intersect the Fast BSS Transition (FT) based solution details.

**4.1:** R0KH position in 802 network:

Some companies believe R0KH location should not be defined in 3GPP, and it is left the implementation.

**Observation 1:** Leaving it to the implementation will not help because if it is not an operator domain or operator has no control on R0KH, then

* debugging will be a challenge
* Auditing will be a challenge
* Responsibility of the issue (who will take a responsibility of the operations issues)

**Observation 2: Issue associated with NSWO based authentication via Fast BSS Transition (FT)**

When there is mobility between two WLAN APs and during the mobility, when there is already de-registration from UDM due to e.g. the UE subscription withdraw or subscription blocked, the authorisation/authentication becomes no longer valid. The WLAN AP, R0KH entity, or UE is not aware of this situation and can still assume that the UE is still authenticated during this mobility. This may lead to the UE to continue using the NSWO based authentication (implicitly) on the new WLAN AP while it shall not be allowed to.

Let's try to understand this by an example:

Step 1: UE is connected to RAN/AMF and authenticated and registered in 5GC.

Step 2: UE connects to WLAN AP#1 and performs NSWO authentication. WLAN AP#1 provides R0KH ID to UE. (See Fast BSS Transition (FT) in 802.11[I] specs)

Step 3: If NSWO-based authentication is successful, then WLAN AP#1 provides the service to UE and stores the security key material in the R0KH holder. WLAN AP#1 also provides R0KH ID and other details to UE..

Step 4: If the UE subscription is withdrawn or UE services are barred in the subscription due to many reasons, the operator stops the UE/SIM services.

Step 5: UDM sends a deregistration notification to AMF to stop the UE services and AMF deregister the UE.

After this, no UE services will be allowed. Even if UE tries to connect or re-register, the primary authentication and/or NSWOF based authentication will fail because UDM will not provide the services(authentication vector) Please refer to TS 33.501, annex S.3.2, step 7 for the details.

But UE is still connected to WLAN AP #1. And R0KH contains the key materials to authenticate the UE in the future.

Step 6: Now UE moves to WLAN AP #2 and provides the R0KH ID received from WLAN AP #1.

Step 7: WLAN AP#2 fetches the context from R0KH and implicitly authenticates the UE.

Step 8: UE continue using the WLAN AP #2 services.

**Observation 3** : Legal issue: even if services are barred for the UE, UE will be authenticated in the next AP (e.g., next hotel) via 5G credentials.

**Proposal:** To avoid both issues, it is proposed to host the R0KH at the AAA proxy. As per TS 23.501, in HPLMN, the NSWOF to WLAN access connection (e.g., SWa’) may be direct, and in other cases, it will be via AAA proxy. Therefore, in HPLMN where, AAA proxy is not deployed, it is recommended to host the R0KH at the NSWOF.  In case of VPLMN where AAA proxy is deployed in VPLMN, the R0KH will be hosted in AAA proxy.

* 
* 

# 5 Conclusions and proposals

Based on the observations made in this paper, we are proposing to agree on **S3-24xx**