**3GPP TSG-SA3 Meeting #102-e *S3-210083***

**e-meeting, 18-29 January 20201**

**Source: NCSC**

**Title: New solution for KI#9**

**Document for: Approval**

**Agenda Item: 5.6**

# 1 Decision/action requested

***It is requested that SA3 approves this new solution for protected transfer of SQNHE across Nudr***

# 2 References

[1] 3GPP TS 33.845, Study on storage and transport of 5GC security parameters for ARPF authentication, v0.3.0

# 3 Rationale

The sequence number SQN­HE­ is part of the *AuthenticationSubscription* data object (3GPP TS 29.505, Clause 5.4.2.2, Table 5.4.2.2-1), and thus can be protected using OAuth tokens in the same way as the long-term key during transfer on Nudr.

# 4 Detailed proposal

START OF CHANGE 1

## 7.x Solution #<x>: Transfer of SQNHE out of UDR

### 7.x.1 Introduction

This solution addresses key issue 9, "protection of sequence number SQNHE during transfer out of UDR".

The solution trusts the access tokens created using the OAuth 2.0 based authorization framework to protect SQNHE from retrieval by unauthorised NFs and to ensure it is only transported along the Nudr interface, along with the TLS protection on the Nudr interface.

This solution is based on capabilities defined or planned to be defined in 3GPP TSs and does not require any additional specification work.

### 7.x.2 Solution details

The OAuth 2.0 based authorization framework defined in 3GPP 33.501[2], clause 13.4.1, is enhanced in Release 16 to support the generation and validation of authorization tokens, including authorization at resource level. This allows the possibility of generating OAuth 2.0 access tokens to restrict retrieval of *AuthenticationSubscription* data to UDM/ARPF NF type service consumers only, preventing unauthorised access by other NF types, for which SQNHE will be transported along the Nudr interface. As with any other SBA reference point, Nudr is protected at transport level using TLS as defined in 3GPP TS 33.501[2] clause 13.1.

### 7.x.3 Evaluation

This solution does not require changes to normative specifications.

END OF CHANGE 1