**3GPP TSG-SA3 Meeting #102-e *draft\_S3-210108-r2***

**e-meeting, 18 – 29 January 2021** *Revision of S3-210108*

**Source: Nokia, Nokia Shanghai Bell**

**Title: Usage of current SBA mechanisms to protect of data in transfer**

**Document for: Approval**

**Agenda Item: 5.16**

# 1 Decision/action requested

***Solution related to KI to eNA study TR33.866 on protection of data in tramsit.***

# 2 References

[1] 3GPP TR 23.700-91: “Study on enablers for network automation for the 5G System (5GS); Phase 2”

# 3 Rationale

UE data is input for analytics generation by NWDAF to be consumed by other NFs. A key issue has been introduced which addresses the security of UE related data transferred between core functions. This contribution argues to use the existing SBA mechanisms to protect data in transit.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\* START OF CHANGES

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |
| --- | --- |
| Solutions | Key Issues |
| 1 Key issues related to securing the data provided to any type of analytics function | 2 Key issues related to detection of cyber-attacks and anomaly events by analytics function | 3 Key issues related to data transfer protection |
|  | 1.1 | 1.2 | 1.X | 2.1 | 2.2 | 2.Y | 3.1 | 3.Y |  |
| #Z: Usage of current SBA mechanisms to protect data in transit |  |  |  |  |  |  |  | X |  |
| #X: <Solution name> |  |  |  |  |  |  |  |  |  |

##

\*\*\*\*\*\*\*\*\*\* NEXT CHANGE

## 6.Z Solution #Z: Usage of current SBA mechanisms to protect data in transit

### 6.Z.1 Introduction

This solution addresses KI#3.Y on protection of data in transfer.

### 6.Z.2 Solution details

Any data transferred between core network functions is protected by SBA mechanisms as described in clause 13.3 and clause 13.4 of 3GPP TS 33.501 [8] for authentication and authorization of NF Service Consumer and NF Service Producer.

According to 3GPP TS 33.501 [8], clause 13.3.0, all network functions shall support mutually authenticated TLS and HTTPS. TLS shall be used for transport protection within a PLMN unless network security is provided by other means. Thus, communication between NFs is integrity, confidentiality and replay protected.

By using an access token issued by NRF, NFs are authorized for requesting analytics from an analytics function or providing analytics data to the analytics function.

Editor's Note: End-to-end integrity and confidentiality protection is FSS.

Editor’s Note: Whether the user consent of data sharing between NFs is mandatory is FFS.

### 6.Z.3 Evaluation

TBD

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