**3GPP TSG-SA3 Meeting #115, AthensS3-24*xxxx***

**26 Feb – 01 Mar 2024**

**Source: Johns Hopkins University APL, US National Security Agency**

**Title:** **Updates to skeleton TR 33.757**

**Document for: Approval**

**Agenda Item: 5.3**

# Decision/action requested

***This pCR is proposing to add a new Key Issue for Server Name Indication extension coordination into TR 33.757***

# 2 References

[1] 3GPP TS 33.210: “Network Domain Security (NDS); IP network layer security”

[2] IETF RFC 6066: “Transport Layer Security (TLS) Extensions”

# 3 Rationale

The purpose of this pCR is to propose adding a new Key Issue for Server Name Indication extension coordination into TR 33.757.

# 4. Detailed proposal

It is suggested to approve the following change.

\*\*\*\* START OF CHANGE \*\*\*\*

# 5 Key issues

5.X Key Issue #X: Server Names coordination between PLMN and NPN customers

5.X.1 Key issue details

TS 33.210 [1] clause 6.2 requires TLS 1.2 clients to support Server Name Indication (SNI) extension as defined in RFC 6066 [2]. PLMN and PNI-NPN TLS configurations will reside in separate operational domains, therefore coordination of the SNI extension is required to ensure the client and server are provisioned with compatible server names across the interfaces between the PLMN and PNI-NPN customer domains.

5.X.2 Security threats

Incompatible SNI extension configuration between PLMN and PNI-NPN customers may result in failure of TLS sessions, thereby exposing PLMN and PNI-NPN customers to operating without the required TLS protections.

5.X.3 Potential security requirements

5GS should include SNI extension coordination across PLMN and PNI-NPN customer domains.

\*\*\*\* END OF CHANGE \*\*\*\*