**3GPP TSG-SA3 Meeting #110Adhoc-e *draft\_S3-231835-r1***

**e-meeting, 17 - 21 April 2023**

**Source: MITRE, Nokia, Nokia Shanghai Bell, Lenovo**

**Title:** **New Key Issue: Support for Policy Decision Points within 5GC SBA**

**Document for: Approval**

**Agenda Item: 5.21**

# 1 Decision/action requested

***This pCR proposes a new KI for TR 33.894: Support for Policy Decision Points within 5GC SBA***

# 2 References

[1] 3GPP TR 33.894 v0.5.0 " Study on applicability of the Zero Trust Security principles in mobile networks"

[2] NIST Special Publication 800-207 Zero Trust Architecture.

[4] 3GPP TR 33.738 v1.0 "Study on security aspects of enablers for network automation for the 5G system Phase 3"

[5] 3GPP TS 33.501 v18.0 "Security architecture and procedures for 5G System"

# 3 Rationale

The Policy Decision Point (PDP) is a logical component defined in [2] and key to an implementation of Zero Trust Architecture (ZTA). In the context of the 5GC, the PDP is responsible for granting, denying, or revoking access to a resource (e.g., NF consumer/Producer, AF) based on current network analytics, external sources, and operator policies*.* This key issue studies the adoption of PDPs within the SBA and the impact on 5G SBA interfaces.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

6.X Key Issue X: Support for Policy Decision Points within 5GC SBA

6.X.1 Key issue details

The Policy Decision Point (PDP) is a logical component defined in [2] and key to an implementation of Zero Trust Architecture (ZTA). In the context of the 5GC, the PDP is responsible for granting, denying, or revoking access to a resource (e.g., NF consumer/Producer, AF) based on current network analytics, external sources, and operator policies*.* This key issue studies the adoption of PDPs within the SBA and the impact on 5G SBA interfaces.

The PDP can aggregate network data and security analytics from various sources including NFs (e.g., NWDAF), AI/ML analytics, or operators/external network security monitoring tools. Based on network status and security analytics the PDP can form dynamic policy to determine the appropriate access control decisions. For example, the NWDAF is used to collect network analytics to detect malicious behaviour from NFs, as is studied in TR 33.738[3] Key Issue #4: Anomalous NF behaviour detection by NWDAF. In this case, the PDP could subscribe to data analytics from NWDAF and when anomalous NF behaviour is detected, the PDP can use these analytics to request re-authentication or allow/deny access to the NF.

The specific policy selection used by PDP will depend on the operator network implementation (e.g., whether NWDAF is deployed). Some example policies can be “request re-authentication after suspicious behaviour detection from NWDAF”, “Only HTTP2 traffic allowed between 5G services”, or any policy that would enforce the requirements from TS 33.501[4] clause 5.9.2 regarding the security requirements on SBA or SBI security in clause 13.

NOTE: How the PDP enforces the policy decisions made, should also be considered in this key issue. In a ZTA, the enforcement of PDP policies is performed by a Policy Enforcement Point (PEP). It is possible for the functions of a PEP to be performed by a Service Communication Proxy (SCP), Network Repository Function (NRF), the NF Producer/Consumer, or a combination of these 5GC components.

Possible applications of PDP to zero trust tenet evaluations from clause 5.1 include Tenet#5 analytics ingestion from other sources (e.g., NWDAF, external security monitoring tools) to inform 5GC security decisions; and Tenet #7 processing of network data to improve policy creation and enforcement in the 5GC.

6.X.2 Security threats

Editor's Note: Details on the threats and attacks are FFS.

6.X.3 Potential security requirements

Editor's Note: Details on the security requirements are FFS.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*