**3GPP TSG-SA3 Meeting #116 *draft\_S3-242429-r3***

Jeju, South Korea, 20th - 24th May 2024 revision S3-241853

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

**Title: New solution for KI#2: Security Policy Enforcement via NRF and SCP/NF**

**Document for: Approval**

**Agenda Item: 5.1**

# 1 Decision/action requested

***This pCR proposes a zero trust policy enforcement approach for TR 33.794[1]: Security Policy Enforcement via NRF and SCP/NF***

# 2 References

[1] 3GPP TR 33.794 Study on enablers for Zero Trust Security

[4] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[11] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

[18] 3GPP TS 23.501: " System architecture for the 5G System (5GS)".

# 3 Rationale

This solution addresses TR 33.794 [1] KI#2 (*Key Issue #2: Security mechanisms for policy enforcement at the 5G SBA)*; Specifically, it addresses *Security policy enforcement Use Case #1: Access control decision enhancement* (i.e., how the data from security monitoring can be considered in access decisions)

This solution proposes to support ZTS policy enforcement in the SBA.

The solution consists of:

1. The NRF subscribes to Operator Security Function (OSF) for operator security policies to grant, deny, or revoke access to a NF Service Consumer, where OSF is outside of 3GPP scope.

This solution describes how to enforce security policy via NRF

# 4 Detailed proposal

SA3 is kindly requested to approve the below change to TR 33.794 [1]

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 7.Y Solution #Y: Security Policy Enforcement via NRF

### 7.Y.1 Introduction

This solution addresses KI#2 (*Key Issue #2: Security mechanisms for policy enforcement at the 5G SBA)*; Specifically, it addresses *Security policy enforcement Use Case #1: Access control decision enhancement* (i.e., how the data from security monitoring can be considered in access decisions)

In the solution the NRF subscribes to Operator Security Function (OSF) for operator security policies to grant, deny, or revoke access to a NF Service Producer, where OSF is outside of 3GPP scope*.*

### 7.Y.2 Solution details



Figure 7.Y.2-1: Security policy enforcement via NRF

1. NF Service Consumer and NF Service Producer perform NF service registration procedure as specified in TS 23.502 [11] 4.17.1.

Note: For brevity, mutual authentication (mTLS) between NFs and other NFs/ SCP/ NRF is not shown in Figure 7.Y.2-1.

1. NRF subscribes to relevant security policy information (e.g., NF Service Consumer/ Producer security posture) via the Operator Security Function (OSF). How the OSF performs the security evaluation of the NF is up to operator. The OSF notifies the NRF when there are changes in the security policy of the relevant NFs.
2. NF service authorization request (i.e., access token request). NF Service Consumer requests authorization from NRF to receive services from an NF Service Producer as described in TS 33.501 [4] clause 13.4. To request the access token NF Service Consumer invokes the Nnrf\_AccessToken\_Get request operation as specified in TS 33.501 [4] clause 13.4.1.1.
3. NRF decides whether NF Service Consumer is authorized to access the requested services.

The NRF uses security policy collected from OSF to determine if there are any security concerns (e.g., anomalous behaviour detected in NF Service Consumer, Expected NF/ NF Service load level) for authorizing the service request.

1. If the service request is authorized, the NRF sends the access token to the NF Service Consumer.

### 7.Y.3 Evaluation

This approach reuses existing functionality for authenticating and authorizing the NF service access request (e.g., TLS, authorization framework in TS 33.501 [4] clause 13.4)

This approach requires new functionality to support:

- NRF subscribes to security policy updates for NFs via the OSF

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*