**3GPP TSG-SA3 Meeting #116 *draft\_S3-242429-r1***

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

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

**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 can be broken into two main parts:

1. The NRF subscribes to Operator Security Function (OSF) for operator security policies to grant, deny, or revoke access to a NF Service Consumer/Producer, where OSF is outside of 3GPP scope.
2. The SCP or NF Producer interfaces with the NRF, and between the NF Service Consumer/Producer to enforce access control policy.

This solution describes how to enforce security policy in direct and indirect communication between NFs.

In direct communication model:

- The NF Service Producer performs security policy enforcement with NRF

In indirect communication model:

- The SCP performs security policy enforcement with 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 and SCP/NF

### 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)

The solution can be broken into two parts:

1. 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*.*
2. The SCP or NF Producer interfaces with the NRF, and between the NF Service Consumer/Producer to enforce access control policy.

### 7.Y.2 Solution details

With NF to NF services direct communication (TS 23.501 [18] Annex E models A or B), there is a direct connection between NF Service Consumer and NF Service Producer (i.e., no SCP). Since this communication does not involve a SCP, the NF Service Producer performs security policy enforcement with NRF.

With NF to NF services indirect communication (TS 23.501 [18] Annex E models C or D), the communication between NF Service Consumer and NF Service Producer is routed through the SCP. In this case, the SCP performs security policy enforcement.

Figure 7.Y.2-1 shows the procedure for direct and indirect communication between a NF Service Consumer and NF Service Producer. To enable ZTS, the authorization framework described in TS 33.501 [4] clause 13.4.1 is used with the additional policy enforcement procedures herein.



Figure 7.Y.2-1: a) Policy enforcement for NF to NF indirect communication with NRF and SCP; b) Policy enforcement for NF to NF direct communication with NRF and NF Service Producer

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.

**Indirect Communication**

1. SCP subscribes to NF security policy updates from NRF for the NF Service Consumer and NF Service Producer (as described in TS 23.502 [11] clause 4.17.7). SCP is notified when there are any changes to the NF Service Consumer or NF Service Producer security policy (e.g., updates, deregistration, security alerts). NRF can trigger notifications in case of security alerts regarding the NF Service Consumer or NF Service Producer based on the security policy subscription in step 1. The SCP can use these alerts to terminate further communication between NF Service Producer and NF Service Consumer.
2. NF Service Consumer sends the service request to the SCP. If delegated discovery is used, then steps 2-4 are performed by the SCP on behalf of the NF Service Consumer.
3. Policy allowing, SCP routes the service request to the NF Service Producer.
4. NF Service Producer authorizes the service request in NF service response by verifying the access token.

The NF service response message is sent to the SCP.

1. SCP routes the NF service response to the NF Service Consumer.

**Direct Communication**

1. NF Service Consumer sends the service request to the NF Service Producer.
2. NF Service Producer subscribes to NF security policy updates from NRF for the NF Service Consumer (as described in TS 23.502 [11] clause 4.17.7). NF Service Producer is notified when there are any changes to the NF Service Consumer security policy (e.g., updates, deregistration, security alerts). NRF can trigger notifications in case of security alerts regarding the NF Service Consumer based on the security policy subscription in step 1. The NF Service Producer can use these alerts to terminate further communication with an NF Service Consumer.

NOTE: Step 6b could happen at anytime to change the policy if NF communications.

1. Policy allowing, NF Service Producer authorizes the service request in NF service response by verifying the access token.

### 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

- NF Service Producers and/or SCP subscribe to security policy updates from the NRF

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