**3GPP TSG-SA3 Meeting #116 *draft\_S3-242423***

Jeju, South Korea, 20th - 24th May 2024 *merger of S3-241717, S3-242296, S3-241852*

**Source: MITRE Corporation, Johns Hopkins University APL, OTD\_US**, **US National Security Agency**, **Nokia, Nokia Shanghai Bell**

**Title: Updates to eZTS Key Issue 2**

**Document for: Approval**

**Agenda Item: 5.1**

# 1 Decision/action requested

***Approve the solution and include in TR 33.794[1]***

# 2 References

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

# 3 Rationale

eZTS [1] has identified Key Issue 2 which looks to find security mechanisms for policy enforcement.

Policy enforcement application requires at least 2 functional entities that can communicate with each other. The first is a function that collects data from one or more sources, processes that data and determines the current security posture based on that data i.e. makes the “decision”. The 2nd function takes the “decision” and executes a defined action. These 2 entities are called the Policy Decision Point (PDP) and Policy Enforcement Point (PEP)[[1]](#footnote-2), respectively.

KI#2 has 2 notes that imply that the operator security function makes decisions and is qualified as the PDP, but there are no requirements for this. While the PDP as described currently in KI#2 is outside the scope of 3GPP, it could be logically broken into smaller functional components. Figure 1 provides a pictorial view.

Diagram

Description automatically generated

Figure – Example in scope/out of scope

**Observation #1: Only the decision-making part of the PDP is outside scope of 3GPP.**

As written above PDP and PEP communicate, there is a need to identify what this communication looks like and to define the attributes and data exchange models.

**Observation #2: What does the communications look like between PDP and PEP and what data needs to be sent from a PDP to a PEP, and vice versa.**

There is also a need to identify where the PEPs are in the SBA. Is there 1, 2 or many? Do they need to communicate between each other or is the communication solely with the PDP.

**Observation #3: PEPs/ PDP should live within the SBA architecture. Define where PEPs / PDP can be placed in the SBA architecture.**

Finally, any communications between PEP and PDP needs to be secure.

**Observation #4: Data-in-transit security is present between the PEP and PDP.**

# 4 Detailed proposal

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

**\*\*\*\*First CHANGE\*\*\*\***

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 33.894, 2023 September, V18.0.0: "Study on applicability of the zero trust security principles in mobile networks", Release 18.

[3] 3GPP SP-231784, "New Study on enablers for Zero Trust Security".

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

[5] RFC 6749, "The OAuth 2.0 Authorization Framework".

[6] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[7] 3GPP TR 33.894, 2023 September, V18.0.0: "Study on applicability of the zero trust security principles in mobile networks", Release 18.

[8] NIST Special Publication 800-207: "Zero Trust Architecture".

[9] 3GPP TR 33.738: "Study on security aspects of enablers for network automation for the 5G system phase 3".

[10] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

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

[12] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[13] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[14] IETF RFC 9113: "HTTP/2".

[15] 3GPP TS 33.117: "Catalogue of general security assurance requirements"

[16] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes

[17] <https://owasp.org/www-community/Threat_Modeling_Process>

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

[x] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3".

**\*\*\*\*End of First CHANGE\*\*\*\***

**\*\*\*\*Second CHANGE\*\*\*\***

## 6.2 Key Issue #2: Security mechanisms for policy enforcement at the 5G SBA

### 6.2.1 Key issue details

Security evaluation and monitoring can enable the identification and potential mitigation of an attack in a 5G network. After the immediate actions on the infrastructure layer such as shutting down relevant virtual machines or containers, long-term actions on the 5G SBA based on operator policies are necessary (e.g., such as updating the NF profiles related to NFs that were affected by the attack).

Updates of the NF profiles are usually done by the NFs itself, using the NRF management services specified in TS 23.502 [11] and TS 29.510 [x], which is not appropriate if the NF itself has been subject to an attack. However, clause 13.4.1.1.1 of TS 33.501 [4] states that "OAuth2.0 clients may also register with the NRF using OAM."

NIST SP 800-207 [8] performs policy enforcement via two functional components, the Policy Decision Point (PDP) and the Policy Enforcement Point (PEP). Policy decisions are made within the PDP while enforcement of a policy is done at the PEP. In the 5GC, policies are the allowed behaviour between NF service producer and NF service consumer and the PDP and PEP help enforce the policy.

### 6.2.2 Security threats

If, for example, the NRF is not updated with information about an NF that has been subject to an attack and mitigations are only performed at infrastructure layers, an attacker could reuse information gained during the attack for extending or re-newing the attack.

### 6.2.3 Potential security requirements

NOTE 1: The logic / policy engine component of the policy decision point (PDP) i.e., Operator’s Security Function, needs to take into account information from layers outside the 3GPP scope and is subject to operators' overall operational security policies, and is hence outside of 3GPP scope. The PDP makes decisions on the security policy, based on attack/threat detection.

NOTE 2: Solutions should take into account the use case described in clause 5.2.1 of the present document.

5GS should support security mechanisms to enable policy enforcement based on the latest security policy (in case any NF is identified as compromised).

**\*\*\*\*End of Second CHANGE\*\*\*\***

1. In some texts a Policy Enforcement Point may also provide data to the PDP so the PEP acts as a data gathering function that then receives instructions to enforce something. [↑](#footnote-ref-2)