**3GPP TSG-CT WG1 Meeting #141eC1-232360**

**Online 17– 21 April 2023**

**Source: Samsung**

**Title: Pseudo-CR on authentication procedures for HTTP request**

**Spec: 3GPP TS 24.542 v0.1.0**

**Agenda item: 18.2.17**

**Document for: Agreement**

**1. Introduction**

This p-CR provide the procedure to authenticate the HTTP requests part of SEAL notification management services

**2. Reason for Change**

The pCR defines the procedures to authenticate a HTTP request received by the notification management server from the notification management client

**3. Conclusions**

It is proposed to agree the following changes to 3GPP TS 24.542 v0.1.0.

\* \* \* 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".

[X] 3GPP TS 24.547: "Identity management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification".

\* \* \* Next Change \* \* \* \*

### 6.2.1 General

#### 6.2.1.1 Authenticated identity in HTTP request

Upon receiving an HTTP request, the SNM-S shall authenticate the identity of the sender of the HTTP request as specified in 3GPP TS 24.547 [X], and if authentication is successful, the SNM-S shall use the identity of the sender of the HTTP request as an authenticated identity.

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