**3GPP TSG-SA WG6 Meeting #69 S6-254404**

**Wuhan, China 13th – 17th Oktober 2025 (revision of S6-254350)**

**Source: Netherlands Police**

**Title: Pseudo-CR on Key issue DM of end-to-end encrypted calls**

**Spec: 3GPP TR 23700-37-030**

**Agenda item: 9.1**

**Document for: Approval**

**Contact: keesdotverweijatpolitiedotnl**

**1. Introduction**

This pCR adds a key issue about performing Discreet monitoring of end-to-end encrypted calls. The text originates from TR 23.784, but has been enhanced as required.

**2. Reason for Change**

This key issue should be addressed in the study.

**3. Proposal**

It is proposed to agree the following changes to 3GPP TR 23700-37-020 v 0.3.0.

\* \* \* First Change \* \* \* \*

## 5.X Key issue X: Discreet monitoring of end-to-end encrypted calls

An authorized MC user may perform discreet monitoring on end-to-end encrypted communications, where those communications can be private calls, individual communications with a server (e.g. pull from or push to a server), and group calls where the target of the discreet monitoring is engaged in group communications. To comprehend the communications, the end-to-end encryption key needs to be available in near-realtime to decrypt the content of the call.

For private or individual communications, a session key is used to encrypt the content of the communications, which is protected in transfer between the call participants by an encryption process making use of the identity of the destination party. The mechanism is described in 3GPP TS 33.180 [6].

For group communications, a GMK is originated by the GMS and protected in transfer to group members one at a time by an encryption process making use of the identity of each group member. The mechanism is described in 3GPP TS 33.180 [6].

According to the requirement in 3GPP TS 22.280 [2] and reproduced in Annex A of the present document, the participants in the call shall not be aware of the discreet monitoring.

Issues:

- To successfully discreet monitor private or individual communications near-realtime access is needed to the session key exchanged between the parties in the private or individual communication. To fulfil the requirement reproduced in Annex A.1, the parties in the call shall not have knowledge of the use of the encryption key for discreet monitoring.

- To successfully discreet monitor group communications near-realtime access is needed to the GMK for the group. To fulfil the requirement reproduced in Annex A.1, the group members in the call shall not have knowledge of the use of the the encryption key for discreet monitoring.

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