**3GPP TSG-SA3 Meeting # 107-e-Ad hoc *S3-221321***

*Was*

**e-meeting, 27th June - 1st July 2022**

**Source:**  **Interdigital**

**Title:** **New key issue on Secure Communication between PINEs**

**Document for: Approval**

**Agenda Item: 5.10**

# 1 Decision/action requested

***It is proposed to approve the key issue described in this document.***

# 2 References

[1] 3GPP TS 23.003: "Numbering, addressing and identification".

[2] 3GPP TR 23.700: “Study on architecture enhancements for Personal IoT Network (PIN) (Release 18)”

# 3 Rationale

According to TR 23.700 [2], PIN ID is defined as Personal IoT Network Identifier. PIN ID is used for identification of PINE, PEGC and PEMC may be managed by 5GS (c.f. clause 5.7).

Per clause 5.4 of the TR 23.700 [2], it is stated that “The PIN connectivity supports communications between PINEs directly, communications between PINEs via PEGC, communications between PINEs via PEGC and 5GS, and

communications between PINE and services outside of the PIN via PEGC and 5GS”.

There is a need for secure communication connectivity between PIN elements (PINEs). This proposal aims to add a new Key Issue on secure communications between PINEs.

# 4 Detailed proposal

\*\*\* 1st 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".

[yy] 3GPP TS 22.261: " Service requirements for the 5G system; Stage 1 (Release 18)".

5.Y Key issue: Secure Communication of PIN

### 5.Y.1 Key issue details

Per clause 5.4 of the TR 23.700-88 [2], it is stated that “The PIN connectivity supports communications between PINEs directly, communications between PINEs via PEGC, communications between PINEs via PEGC and 5GS, and communications between PINE and services outside of the PIN via PEGC and 5GS”.

In clause 6.38.2.6 of the TS 22.261 [yy], the following requirement is indicated:

"The 5G system shall provide user privacy; location privacy, identity protection and **communication confidentiallity for non-3GPP devices and UEs** that are using the PIN Element with Gateway Capability, eRG or PRAS."

There is a need for secure communications between PIN elements, and deployment of PEGC shall not reduce security of communication between PIN elements.

### 5.Y.2 Security threats

TBD.

### 5.Y.3 Potential security requirements

TBD.

\*\*\* END OF CHANGES \*\*\*