**3GPP TSG-SA3 Meeting # 107-e-Ad hoc S3-221319**

 *Was*

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

**Source:**  **Interdigital**

**Title:** **New key issue on Protecting Identification of PIN and PIN Privacy**

**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

Per clause 5.7 TR 23.700 [2, “Whether and what characteristics of a PIN shall be known to the 3GPP network (e.g. type of PIN (wearable, home automation, factory etc.), max of PIN elements in the PIN, etc.). How to support identifying PINE, PEGC and PEMC, and whether and how the 5GS manages the identifier.”

This pCR proposes a new Key Issue, Protecting Identification of PIN and PIN Privacy.

# 4 Detailed proposal

\*\*\* 1st CHANGE \*\*\*

5.Y Key issue: Privacy protection of PIN

### 5.Y.1 Key issue details

According to TR 23.700-88 [yy], some information have privacy concern, for example, all kinds of identifiers for PIN that may be managed by 5GS, such as PIN ID, which is defined as Personal IoT Network Identifier, PINE/PEGC/PEMC ID, which is used for identification of PINE, PEGC and PEMC, other examples like password for accessing a PIN, SSID/BT ID of a PEGC, etc.

Per clause 5.7 TR 23.700-88 [yy], “Whether and what characteristics of a PIN shall be known to the 3GPP network (e.g. type of PIN (wearable, home automation, factory etc.), max of PIN elements in the PIN, etc.). How to support identifying PINE, PEGC and PEMC, and whether and how the 5GS manages the identifier.”

Editor’s Note TR 23.700 [yy]: Security and privacy aspects of PIN identifier is FFS and is left to SA WG3.

### 5.Y.2 Security threats

An attacker eavesdropping on information with privacy concern used inside and outside PIN, and is capable of the following privacy attacks:

- inferring the information of PIN,

- inferring PINEs, PEGC, and PEMC presence in the corresponding area,

- tracking the PINEs, PEMCs and PEGCs.

- accessing the PIN.

### 5.Y.3 Potential security requirements

The 5G system should provide means to protect privacy on information provisioned by PEMC to network, or provisioned from network to PINE, PEGC, PEMC.

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