**3GPP TSG-SA3 Meeting # 108-e S3-221784-r2**

 *Was*

**e-meeting, 22 – 26 August 2022**

**Source:**  **Interdigital**

## **Title:** **New key issue on Secure policy and parameters provisioning for PIN**

**Document for:** **Approval**

**Agenda Item:** **5.10**

# 1 Decision/action requested

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

# 2 Rationale

There is a need for secure provisioning of policy and parameters for a PIN. This PCR proposes a new KI aiming to study secure provisioning of policy and parameters for a PIN.

# 3 Detailed proposal

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

## 5.Y Key issue: Secure policy and parameters provisioning for PIN

### 5.Y.1 Key issue details

Per clause 5.6 of TR 23.700-88 [2], “The necessary secure policy/parameters configuration are needed for the communication between PINEs, PINE/PEGC/PEMC discovery, authorization for PINE/PEGC/PEMC.”

Furthermore, per TR 23.700-88 [2], clause 6.0D.2.3, “The PIN Application Server (PIN AS) is an optional NF and includes AF functionality can be deployed by mobile operator or an authorized third party. PIN AS may support Configuration and parameters provisioning to PEGC, PEMC, PINE”.

### 5.Y.2 Security threats

An attacker can compromise the necessary procedures, e.g., communication between PINEs, PINE/PEGC/PEMC discovery and will be vulnerable to the following security attacks:

- compromised policy configuration of PINEs’ membership in PIN, which as a result may compromise the security of relevant procedures (discovery, authorization, communication)

### 5.Y.3 Potential security requirements

The 5G system should provide the means to securely provision PIN policy/parameters configuration to PEGC, PEMC, PINE for the PIN service.

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