**3GPP TSG-SA3 Meeting # 108-e S3-221782**

 *Was*

**e-meeting, 22 – 26 August 2022**

**Source:**  **Interdigital**

**Title:** **New subclause - Assumptions for PIN**

**Document for: Approval**

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

# 1 Decision/action requested

***It is proposed to approve the subclause proposed in this document.***

# 2 Rationale

This contribution adds a subclause to the existing clause Assumptions to define the main properties of PINs that may affect PIN security and privacy.

# 3 Detailed proposal

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

4 Assumptions

4.1 Important properties of PINs potentially affecting PIN security and privacy

The following is the unprioritized list of PIN properties:

Battery-powered: The nodes in a PIN are typically mobile PINEs. They are often not connected to a power supply and have to draw their energy from a battery. To avoid battery exhaustion in a short time, the intensive use of expensive operations (from an energy point of view) has to be minimized. Mobile PINEs with limited resources go into sleep mode from the moment they do not have to send or receive data. Always being online may consume too much energy.

Dynamic network topology: The nodes in a PIN are often mobile. Such PINEs can move from one place to another. They can go offline to preserve energy or because they are not operated by the user at that moment. Because of these reasons, the network topology is dynamic. The number of PINEs in the network can change in place and time. The lifetime of a PIN can be short. Connections are established on the spot. From the moment the data transfer has finished, the PINEs may disconnect.

Heterogeneity: The PINEs that can make up the Wireless Personal Area Network can have very different capabilities. This can range from a laptop (having rather large energy and computation resources) to a smartwatch (being battery-powered and having limited computational power).

Limited range: The range of a Wireless Personal Area Network is determined by the antenna and wireless radio configuration of the mobile device. Typically, the range is a few meters. The communication in a PIN is therefore most of the time over a single hop. A PINE communicates directly to the intended destination, which is in the sending range. It is however possible to extend the range of a PIN and send data to PINEs outside of the single-hop range. Wireless Personal Area Networks can be grouped in clusters to form a larger network (e.g., scatter-nets in the Bluetooth standard). In this case, the data is forwarded from hop-to-hop (multi-hop communication).

Wireless: A PIN is in all practical cases wireless, since wiring limits the mobility of the PINEs in the network. The data is transmitted via the wireless radio. Since wireless communication does not stop at the destination, a passive eavesdropper located within receiving range can receive all transmitted data.

A small number of PINEs: Since a Wireless Personal Area Network is centered around a single or a small number of users, the number of PINEs in the network is typically very low. E.g., Bluetooth PINEs can form pico-nets, which consist of at most 8 PINEs. Often, the number of PINEs will be even smaller (two or three PINEs that need to exchange some data).

User-operated: Most PINEs in the PIN (e.g., a handset, or laptop) are operated by a user or a small number of users or use autonomous/programmable operation.

Providing security for PINs is essential as wireless links are easy to eavesdrop on undetected. PINs need a security architecture that provides the confidentiality and integrity of messages, mutual data and entity authentication, location privacy, and availability. Due to the specific properties of PINs, it is not straightforward to provide these security services.

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