**3GPP TSG-SA WG1 Meeting #92e S1-204059r01**

**Electronic Meeting, 11-20 November** *(revision of S1-20xxxx)*

Title: PINs –onboarding

Agenda Item: 7.12.1 - FS\_PINs

Source: vivo Mobile Communications Ltd,

Contact: Adrian Buckley <adrian.buckley@vivo.com>

*Abstract: This contribution proposes to add onboarding material and potential requirements*

# Discussion

A PIN user is able to create a PIN. A user could purchase a headset and want to listen to music from their smartphone. There might be no cellular coverage when they decide to perform this action so it should be possible to allow a PIN to be created when there is no coverage. In such circumstances such devices should only be allowed to use none operator managed spectrum as an operator is usually responsible for devices that operate within spectrum they have a license for. None operator managed spectrum may also become “crowded” with devices so there should be an option to use operator managed spectrum, in this situation connectivity will be required to the operators network so that the operator can authenticate and authorise a device.

When a PIN user creates a PIN there could be many devices within that PIN that can do a variety of tasks. Some of these tasks might be ok with latency and other tasks not. A PIN could be large in terms of devices so there is a need to “manage” policies for PIN devices. PIN devices also need to be able to communicate is a secure fashion, however as illustrated above a PIN can be created when there is no cellular coverage so there needs to be a way to create a secure connection in these circumstance, however if cellular connectivity exists it should be possible to improve the security. A third party should be able to update a PINs authentication / encryption credentials to be more secure, in addition if a PIN device uses operator managed spectrum the credentials should be managed by the operator so that they can manage the policy of the device and stop it using operator managed spectrum if required.

**\*\*\*\*First CHANGE \*\*\*\***

### 5.1.3 Service Flows

#### 5.1.3.1 General

Florence (PIN-User) has decided to build a home automation network (PIN) and has purchased a number of devices i.e. some light bulbs, power sockets, a gateway that acts as a voice assistant and door / window sensors (these are known as PIN Devices). The instructions on the PIN Devices indicate that the PIN Device should be no more than 100m direct line of sight from the PIN device managing the PIN however this might be affected by walls, furniture etc. To improve connectivity some PIN Devices can help extend coverage of the PIN e.g. relays (PIN Relay). The light bulbs and power sockets indicate that these devices can help extend the coverage and that the purchaser should position them around their house / condominium so that devices that cannot communicate directly with the device acting as a gateway can use multiple relays if necessary. PIN relays can also be daisy chained together to greatly improve coverage. Florence provisions her PIN Devices into the PIN Device that manages the PIN. Checking her APP she sees one of the PIN Devices, a door sensors, is offline. She moves a PIN Device that acts as a relay, smart light bulb, and then opens and closes the door and sees in real time the door sensor reports the action. A while later her son turns the light switch off as he sees it in the wrong position. Later that day Florence sees the PIN Device, door sensor, offline again and finds out her son turned the light switch off. She decides to install a smart light switch near the door sensor to prevent that issue from occurring again. Florence speaks to the voice assistant that turns the light bulbs on and off in real time. The door sensor reports when the door is opened and closed with notifications on her smartphone in real-time. Later Florence install a smart door lock on the door with the door sensor. The door lock created a secure connection with the PIN. When she activates the door to open using her app she notices it takes a second before the bolt moves.

When Florence installs a new PIN Device into the PIN the instructions indicate that the PIN Device that manages the PIN has to be within 2m so that the 2 PIN Devices can successfully communicate. After that a PIN device may use a PIN device that extends the PIN network coverage to successfully communicate with the PIN device that manages the PIN.

#### 5.1.3.2. Onboarding

When Florence first setup her PIN she had one device that was designated as a gateway. She is aware of the following capabilities of the gateway (it is in the instruction manual and available by the UI). Florence also configures one PIN device to be able to adds subsequent PIN Device to the PIN by scanning in a QR or bar code from the device.

NOTE: Other methods could be possible whereby Florence needs to type in information including encryption keys. This could be by the authorised PIN device (e.g. smartphone) or a UI etc. on the gateway.

She knows that the PIN device that needs to be added has to be within communications range of the gateway device (i.e. no relay devices can be used yet) so that it can be provisioned into the PIN. Florence is aware that she can provision devices without the getaway having a direct network connection connectivity, but direct network connection connectivity will give her the option to:

a) allow her PIN to be more secure; and

b) if a PIN device, if it supports the capability, to have a better user experience e.g. security equipment, door locks have guaranteed real time operation.

This later feature, b), requires Florence to call her service provider to activate the capability. The service provider also provides a service that allows Florence to easily move a PIN device from using one gateway to another gateway. Service provider services are flat rate or volume charged (e.g. data size, number times operation occurs).

Florence also has the option to allow which PIN devices can interact with other PIN devices via the UI of the PIN device that acts as a gateway.

### 5.1.4 Existing features partly or fully covering the use case functionality

See sub-clause 5.5.5

### 5.1.5 Potential Functional Requirements

[PR 5.1.5-1] The 5G system shall support the ability to create a Personal IoT Network.

[PR 5.1.5-2] A PIN shall support both delay and non-delay tolerant services. Maximum delay for non-delay tolerant services shall be 200ms [4] from the sending PIN Device to the receiving PIN Device (e.g. ask the voice assistant [sending PIN Device] to turn a light on [receiving PIN Device]).

[PR.5.1.5-3] A user of a PIN shall be able to construct a fault tolerant PIN so that no single failure shall result in a loss of connectivity.

 [PR.5.1.5-4] The PIN shall support a PIN device that acts as a gateway. The gateway shall be able to perform the following when it supports direct device connection using non licenced spectrum:

i) provides connectivity to the internet either directly and or via 3GPP wireless access using direct network connection;

ii) uses direct device connection to communicate with a PIN Device in the home / garden / yard;

iii) acts as the entity that manages the PIN, managing the PIN includes:

1. Authenticate and authorise a PIN device into the PIN network;

NOTE 1: This capability is also possible when the PIN device acting as a managing entity for the PIN has no connectivity outside of the PIN. In this situation it may mean that authentication credentials etc. are not as strong if connectivity outside of the PIN (e.g. via direct network connectivity) was possible.

1. Stores PIN device credentials (identity, authentication, encryption etc. information) when using non licensed spectrum;
2. What the PIN device is authorised (Policy) to do;

1. If a PIN device, including which one, can add other PIN devices to the PIN.

2. Connection technology and band information a PIN device is allowed to use.

NOTE 2: The gateway has to prevent PIN devices operating in operator managed spectrum.

3 If a PIN device can use a 2nd or 3rd PIN concurrently or not.

NOTE 3: There is a need to keep track of the other PINs being used.

1. How each PIN device can be reached within the PIN e.g. via relay a; relay b and relay c etc.
2. latency requirements of a PIN device,

[PR.5.1.5-5] When a PIN device that acts as a gateway UE supports direct network connection, the gateway shall, in addition to those items listed in [PR.5.1.6-4]

a) When authorised by an operator allow a PIN device to use direct device connection using licenced spectrum.

When a PIN device uses licensed spectrum the credentials used by the PIN device shall be managed by the operator.

NOTE: Authorisation by an operator could mean that the gateway UE acts as a relay and forwards the operator authorisation from the 5G system.

b) If the gateway UE loses connectivity to the 5G system the gateway UE needs to prohibit a UE from using licensed spectrum.

c) Store, support authentication and encryption credentials provided by an authorised 3rd party when the PIN device uses non licensed spectrum.