3GPP TR 22.859 V1.1.0 (2021-05)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Study on Personal Internet of Things (PIoT) networks

(Release 18)

** 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.  
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.  
This Report is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

5G, Network Slice

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

***Copyright Notification***

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2021, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword 6

1 Scope 7

2 References 7

3 Definitions and abbreviations 8

3.1 Definitions 8

3.2 Abbreviations 8

4 Overview 9

5 Use cases 10

5.1 Traffic Scenario: inHome 10

5.1.1 Description 10

5.1.2 Pre-conditions 11

5.1.3 Service Flows 12

5.1.3.1 General 12

5.1.3.2. Onboarding 13

5.1.4 Existing features partly or fully covering the use case functionality 14

5.1.5 Potential Requirements 14

5.1A The lost dog 15

5.1A.1 Description 15

5.1A.2 Pre-conditions 16

5.1A.3 Service Flows 16

5.1A.4 Post-conditions 17

5.1A.5 Existing features partly or fully covering the use case functionality 17

5.1A.6 Potential New Requirements needed to support the use case 18

5.2 Positioning with VR and AR 18

5.2.1 Description 18

5.2.2 Pre-conditions 18

5.2.3 Service Flows 19

5.2.4 Post-conditions 19

5.2.5 Existing features partly or fully covering the use case functionality 19

5.2.6 Potential New Requirements needed to support the use case 19

5.3 Media share within PINs Use case 19

5.3.1 Description 19

5.3.2 Pre-conditions 20

5.3.3 Service Flows 20

5.3.4 Post-conditions 21

5.3.5 Existing features partly or fully covering the use case functionality 21

5.3.6 Potential New Requirements needed to support the use case 21

5.4 Switching between non-3GPP RAT and 3GPP RAT direct device connections Use case 22

5.4.1 Description 22

5.4.2 Pre-conditions 22

5.4.3 Service Flows 22

5.4.4 Post-conditions 23

5.4.5 Existing features partly or fully covering the use case functionality 23

5.4.6 Potential New Requirements needed to support the use case 23

5.5 Use case: UE accessing Services provided by PIN Elements behind 5G enabled gateway(s) 23

5.5.1 Description 23

5.5.2 Pre-conditions 25

5.5.3 Service Flows 25

5.5.4 Post-conditions 26

5.5.5 Existing features partly or fully covering the use case functionality 27

5.5.6 Potential New Requirements needed to support the use case 27

5.6 UE accessing PIN applications hosted by a PIN Element with Gateway Capability 28

5.6.1 Description 28

5.6.2 Pre-conditions 29

5.6.3 Service Flows 29

5.6.4 Post-conditions 29

5.6.5 Existing features partly or fully covering the use case functionality 29

5.6.6 Potential New Requirements needed to support the use case 30

5.7 Tour Guide Use case 30

5.7.1 Description 30

5.7.2 Pre-conditions 31

5.7.3 Service Flows 31

5.7.4 Post-conditions 32

5.7.5 Existing features partly or fully covering the use case functionality 32

5.7.6 Potential New Requirements needed to support the use case 32

5.8 Use case support of broadcast-based service discovery 32

5.8.1 Description 32

5.8.2 Pre-conditions 33

5.8.3 Service Flows 33

5.8.4 Post-conditions 33

5.8.5 Existing features partly or fully covering the use case functionality 33

5.8.6 Potential New Requirements needed to support the use case 33

5.9 Adding personal health devices to PIN 34

5.9.1 Description 34

5.9.2 Pre-conditions 34

5.9.3 Service Flows 34

5.9.4 Post-conditions 35

5.9.5 Existing features partly or fully covering the use case functionality 35

5.9.6 Potential New Requirements needed to support the use case 35

5.10 Personal health monitoring PIN Elements 35

5.10.1 Description 35

5.10.2 Pre-conditions 36

5.10.3 Service Flows 36

5.10.4 Post-conditions 37

5.10.5 Existing features partly or fully covering the use case functionality 37

5.10.6 Potential New Requirements needed to support the use case 37

5.11 Dynamic creation of an on-demand PIN at home 37

5.11.1 Description 37

5.11.2 Pre-conditions 38

5.11.3 Service Flows 38

5.11.4 Post-conditions 39

5.11.5 Existing features partly or fully covering the use case functionality 39

5.11.6 Potential New Requirements needed to support the use case 39

5.12 Operator managed PIN 39

5.12.1 Description 39

5.12.2 Pre-conditions 39

5.12.3 Service Flows 40

5.12.4 Post-conditions 40

5.12.5 Existing features partly or fully covering the use case functionality 40

5.12.6 Potential New Requirements needed to support the use case 40

5.13 A smart hospital bed as a PIN element 40

5.13.1 Description 40

5.13.2 Pre-conditions 41

5.13.3 Service Flows 41

5.13.4 Post-conditions 42

5.13.5 Existing features partly or fully covering the use case functionality 42

5.13.6 Potential New Requirements needed to support the use case 42

6 Considerations 42

7 Potential Consolidated Requirements 42

7.1 Gateway 42

7.2 Service Discovery 43

7.3 Service Hosting 43

7.4 Privacy 43

7.5 Direct Communications 43

7.6 Connectivity - QoS - charging 43

7.7 Provisioning 44

7.8 Positioning 44

7.9 KPIs 44

8 Conclusions and Recommendations 44

Appendix A Connectivity models 45

A.1 General 45

A.2 PIN direct connectivity with no relay 45

A.3 PIN direct connection using a relay. 46

Annex A: Change history 47

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

# 1 Scope

The present document is aiming at documenting potential new use cases and service requirements to enhance 5GS for the support of Personal IoT networks (PINs), including when the PIN is connected to 5GC.

# 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".

[2] 3GPP TS 22.261: "Service requirements for the 5G system".

[3] 3GPP TS 22.101: "Service principles".

[4] Christiane Attig, Nadine Rauh, Thomas Franke, & Josef F. Krems (May 2017) "System Latency Guidelines Then and Now – is Zero Latency Really Considered Necessary?  
<https://www.researchgate.net/publication/317801643_System_Latency_Guidelines_Then_and_Now_-_Is_Zero_Latency_Really_Considered_Necessary/link/5ae18fc4458515c60f662370/download>

[5] 3GPP TS 22.278: "Service requirements for the Evolved Packet System (EPS); Stage 1".

[6] 3GPP TR 22.858: " Study of Enhancements for Residential 5G; Stage 1".

[7] 3GPP TS 22.115: “Service aspects; Charging and billing”.

[8] 3GPP TS 22.228: "Service requirements for the IP multimedia core network subsystem".

[9] ZigBee® Specification  
<https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf>

[10] Z-Wave® Specifications  
https://z-wavealliance.org/z-wave-specifications/

[11] 2020 US Census  
<https://www.census.gov/construction/chars/highlights.html#:~:text=The%20median%20size%20of%20a,house%20was%202%2C301%20square%20feet>.

[12] Minimum provision of electrical Socket-outlets in the home  
<https://www.electricalsafetyfirst.org.uk/media/1204/guidance-on-minimum-provision-socketsv2.pdf>

[13] David Wilson Homes  
<https://www.dwh.co.uk/advice-and-inspiration/average-house-sizes-uk/#:~:text=Average%20UK%20house%20size%3A%20656%20sq>.

[14] National Electrical Code 70®  
<https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=70>

[15] 3GPP TR 22.104: "Service requirements for cyber-physical control applications in vertical domains; Stage 1".

[16] <http://www.slatools.com/sla-uptime-calculator#:~:text=Uptime%20is%20the%20amount%20of,and%2050%20seconds%20of%20downtime>.

[17] USATODAY 17th Dec 2020  
<https://www.usatoday.com/story/tech/columnist/komando/2020/12/17/amazons-sidewalk-shares-internet-connection-you-may-want-opt-out/3887227001/>

[18] https://forge.etsi.org/rep/ITS/asn1/ieee1609.2/blob/1609.2-etsi2020/Ieee1609Dot2BaseTypes.asn

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**direct device connection:** See definition in TS 22.261 [2].

**direct network connection:** See definition in TS 22.261 [2].

**Guest PIN Element:** Is a PIN Element that is a member of one PIN (Home PIN) and can access any other PIN, if allowed to by that PIN to communicate with the Home PIN.

**IoT device:** See definition in TS 22.261 [2].

**PIN direct connection:** the connection between two PIN Elements without any 3GPP RAN or core network entity in the middle.

NOTE 1: A PIN direct connection could internally be relayed amongst other PIN Elements.

NOTE 2 When a PIN direct connection is between two PIN Elements that are UEs this direct connection is typically known as a direct device connection as defined in TS 22.261 [2].

**PIN Element:** UEs and devices authorised to communicate within a PIN.

**PIN Element with Gateway Capability:** a UE PIN Element with the ability to provide (for other PIN Elements) or indirect Network connection (for other PIN Elements) to and from the 5G network.

NOTE 3: A PIN Element can have both PIN management capability and Gateway Capability.

Editor’s Note: The relationship with FS\_RESIDENT Evolved Residential Gateway will be resolved in the normative phase.

**PIN Element with Management Capability:** A PIN Element with PIN management Capability has capability to manage the PIN.

**Personal IoT Network:** A configured and managed group of at least one UE and one or more PIN Elements or UEs that are (pre-)authorised to communicate with each other.

NOTE 4: The configuration and management of the PIN can be maintained locally or by the 3GPP network.

**PIN-User:** The PIN-User is the person who owns the PIN with respective subscriptions at one service provider.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

PIN Personal IoT Network

UPnP Universal Plug and Play

DNLA Digital Living Network Alliance

# 4 Overview

IoT capabilities have been designed for devices that communicate using the traditional cellular network, including battery constrained devices where it is expected that the battery should last in the order of years. Recently standards have been extended to support more vertical IoT devices for factory based, audio visual, medical, mission critical and vehicular solutions. In some contexts, e.g. factory based solutions the concept of a private network has been introduced, this has the added benefit for devices that generate very little user plane traffic (e.g. sensors etc.) the traditional cellular operator might not have to dedicate resources to them in the network and the traffic can stay within the local “factory (private network) environment”. There are 2 consumer segments that have similar traffic characteristics where private networks provide an advantage, where communications are predominately within the constraints of a localized IoT network:

i) Wearable devices;

ii) Home automation

For the purpose of this discussion these will be called “Personal IoT networks” (PINs). These types of networks are very different to commercial IoT device, they are usually less rugged, most highly battery constrained and lifespan of the battery typically a couple of days or weeks. User plane traffic typically stays with a constrained environment, around the body or in the home i.e. within the PIN. Notifications can be received on smartphones that events have occurred within the PIN.

PINs have been around for a long time using others standards however their take up / adoption rate has been low compared to the general smartphone UE.

a) An example of a home automation PIN can be seen in Figure 4-1 where there are a number of devices in the home that either communicate directly with the hub or indirectly via a relay to the hub. A smartphone in the 5G system can receive notifications regarding events (e.g. door opens) from the home automation PIN.

NOTE 1: The diagram shows home automation but it could equally be a smart office environment, smart police or fire station etc.

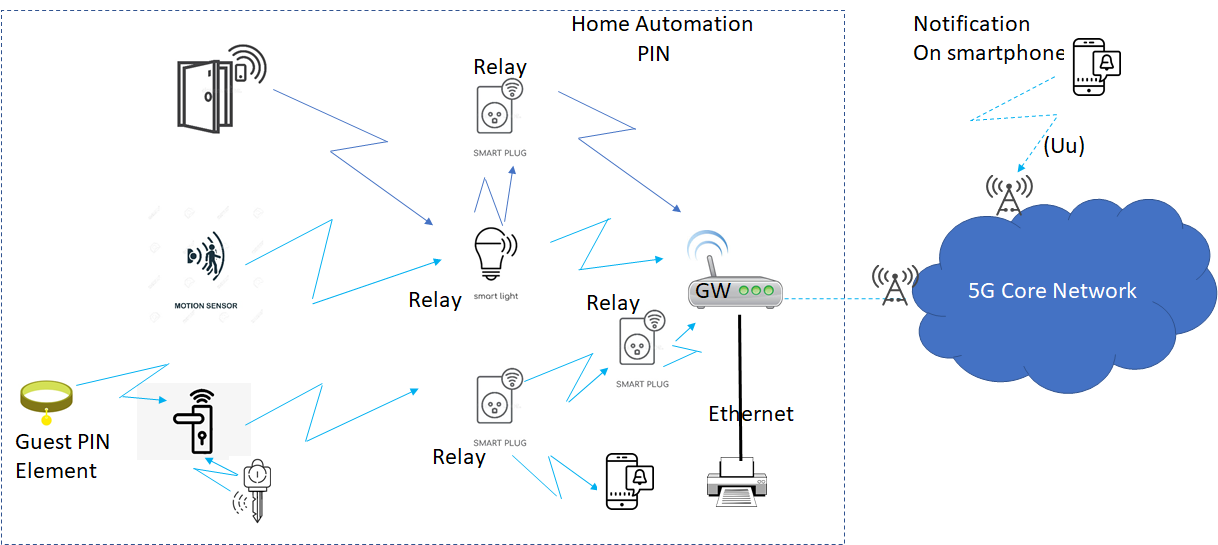


Figure 4-1: Home automation PIN

b) Wearables can use a multitude of different access technologies, battery life can in some situations be severely constrained just by the physical dimension limitations e.g. glasses frames, earbuds, blood pressure monitor, pacemaker and rings. Space is also at a premium, capabilities are limited (memory, processing power, even USIM functionality might not be available). Location requirements on wearable devices, especially those with Uu interfaces can contribute to battery drain. Earbuds / Rings are very small, even an ESIM chip takes up valuable space, battery consumption and adds weight to the device. Figure 4-2 shows two wearable networks, one where all the devices communicate via the smartphone and another where glasses act as a relay for smart earbuds.

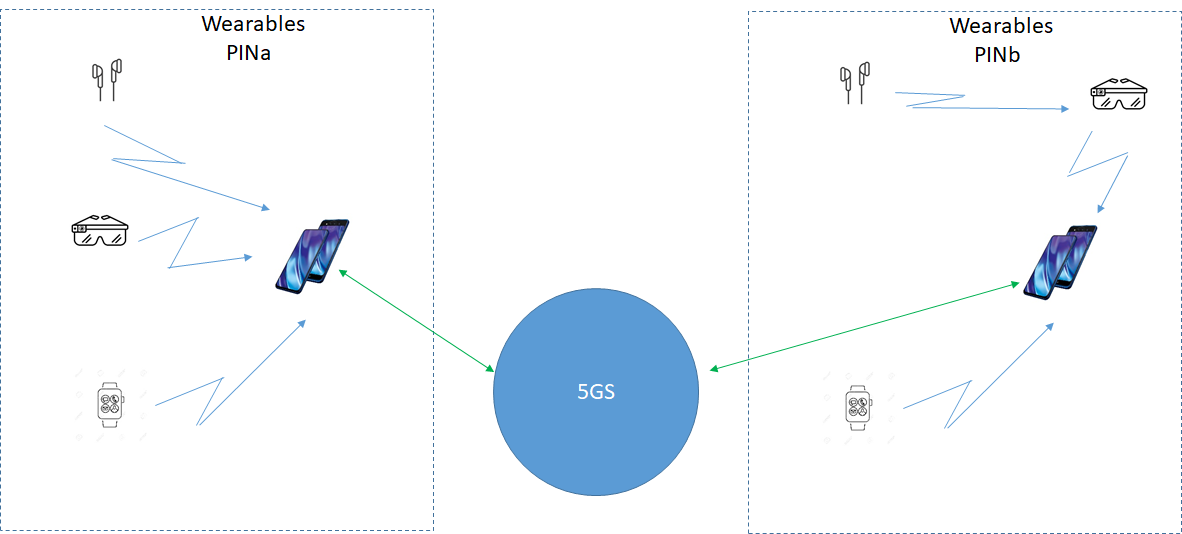


Figure 4-2: Wearable PINs

NOTE 2: The diagram shows wearable networks as used today by consumers, a wearable network could also be employed in industrial, medical or even first responder situations.

In summary, it is considered beneficial for 3GPP specification to address 5G system support of different use cases for PINs.

# 5 Use cases

## 5.1 Traffic Scenario: inHome

### 5.1.1 Description

Houses, offices, light industrial have many opportunities to be automated, the traditional light bulbs, power sockets, thermostats, sprinkler systems, leak detection and the new smart appliances such as ovens, washing machines, faucets etc. can communicate with each other via a Personal IoT Network (PIN). These devices, to be known as PIN Elements, can have the following characteristics:

i) some have continuous power and others don’t;

ii) some have strict latency requirements e.g. items that are part of an alarm system, while others provide delay tolerant data;

iii) some need to perform an action so an individual sees an action as instantaneous (e.g. ask the voice assistance to turn the light bulb on and its appears instantaneous); and

iv) need to perform an action but they don’t have strict latency requirements e.g. sprinklers need to come on but it doesn’t matter if its few seconds late.

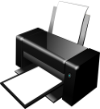
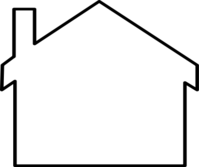
The PIN Elements listed above and many others that are not listed above can communicate with hubs / gateways within the PIN where some control can take place at the gateway (e.g. thermostats and sprinkler controllers are usually self-contained within the PIN Element, whereas power sockets and light bulbs might communicate with a PIN Element that manages the PIN that control their actions). In addition, thermostats etc. can also communicate with these PIN Elements that manage the network known as PIN Element with Management Capability. Power sockets, light bulbs and switches can also act as relay type devices extending the coverage of the PIN.

NOTE 1: A thermostat controller may have remote sensors that communicate with the thermostat. Effectively there can be a PIN within a PIN.

In case of the PIN Element that provides access to the 5GS, known as PIN Element with Gateway Capability (shown as a GW in Figure 5.1.1-1) these could be placed in one corner of the house.

NOTE 2: The PIN Element with Gateway Capability in this diagram also manages the PIN and also is a PIN Element with Management Capability.

When planning a network in a house many houses suffer from problems of coverage due to the number of floors and other obstacles (i.e. walls, doors, columns, furniture), users will plan or configure their PIN Networks based on their needs and may install or move PIN Elements. When the PIN Element with Management Capability connects to a broadband (also acting as a PIN Element with Gateway Capability) network most houses have only one entry network point where the PIN Element with Gateway Capability can be installed.



GW

5G

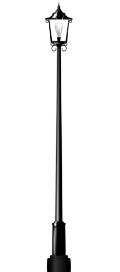
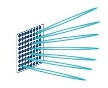


Figure 5.1.1-1: inHome scenario

Furthermore, with the use of millimetre waves there is the danger that the signal is blocked even by people while moving and alternative connection paths are needed. Therefore, enhanced "fully meshed relays" will play a key role in achieving extensive fault tolerant coverage in inHome scenarios. These fully meshed relays allow the resident of the home to position relays (PIN Elements) to create a network that is fault tolerant e.g. should a relay fail, devices such as those that detect motion or a door opening can still reach the PIN Element with Management Capabilities. Data is encrypted from the end device to the PIN Element with Management Capabilities.

NOTE 3: It is up to the home resident to plan their network accordingly so a single failure in the PIN does not stop a PIN Element communicating with any other PIN Element. The home resident is aware that certain types of devices can act as relays.

### 5.1.2 Pre-conditions

Let’s consider an average house can be around 100m2-120m2 with 3 floors. Regarding devices and applications within the home we can categorize them in the following groups:

a) Lighting, appliances, sockets and climate control: This is the traditional home automation and control network where continuous power is available to each PIN Element. These PIN Elements can act as fully mesh relays due to being continually powered. Their time to change state (e.g. light bulb from off to on) needs to occur within 200ms [4].

b) Security Systems: This includes traditional security components such as motion detector, door / window sensors, automatic lock (PIN Elements). These items are battery powered, in case of door / window sensors it can be expected that the battery should last for 2+ years. Due to nature of these PIN Elements the delay to inform the PIN Element with Management Capabilities that an event has occurred needs to be 200ms [4]. Some devices will need to rely on mesh relays for routing their data. PIN Elements that are also critical to life and safety e.g. motion sensors, alarms, door locks, alarm systems etc can only been offline for seconds a week. Using an availability calculator [16] 99.999% equates to 1 second or less per day.

PIN-user is aware that they need to plan their network (PIN) and walls, doors etc can present challenges to planning a network. Given PIN Elements can be moved the configuration of a network can change e.g. PIN Element A might have used PIN Element B and Element C as relays however PIN Element B is moved and thus the user who created the PIN needs the PIN Elements within the PIN to discover the network configuration/layout/plan has changed. A user can request the PIN to perform a network configuration/layout/plan test to see what PIN Elements can communicate with other PIN Elements with or without relays.

PIN-user is aware which PIN Elements can act as a relay and which ones cannot.

Some example dimensions of products PIN Elements are:

I Light switch: 1.76 x 2.2 x4.1 inches (USA), 86 x 86 x 41 mm (EU);

II Power outlet: 1.75 x 2.1 x 4.2 inches (USA), 86 x 86 x 50 mm (EU);

III Motion sensor: 18 x 71 x 19 mm, Battery ER14250[[1]](#footnote-1);

IV Light bulb: 3 x 4.9 x 3 inches (USA), 6.5 × 6.5 × 14 cm (EU).

A PIN has at least one PIN Element with Management Capabilities. This PIN Element contains a list of PIN Elements that are in the PIN, what each PIN Element is allowed to do (act as a relay in the PIN, end device), if the PIN Element can be communicated with and what credentials they use to access the PIN. A PIN Device may be used to provision each PIN Element in the PIN Element that manages the PIN (PIN Element with Management Capabilities). The PIN Element with Management capability will need to know information about a PIN Element, some attributes could include:

- Unique identifier for the PIN Element within that PIN;

- Application(s) (e.g. Application ID) hosted on the PIN Element;

- PIN direct connections types supported by a PIN Element

- Metadata associated with the application (e.g. event has occurred, type of event, timestamp etc);

- Security credentials;

Approximate no more than [500] bytes of data.

PIN Elements use PIN direct connections to communicate with each other.

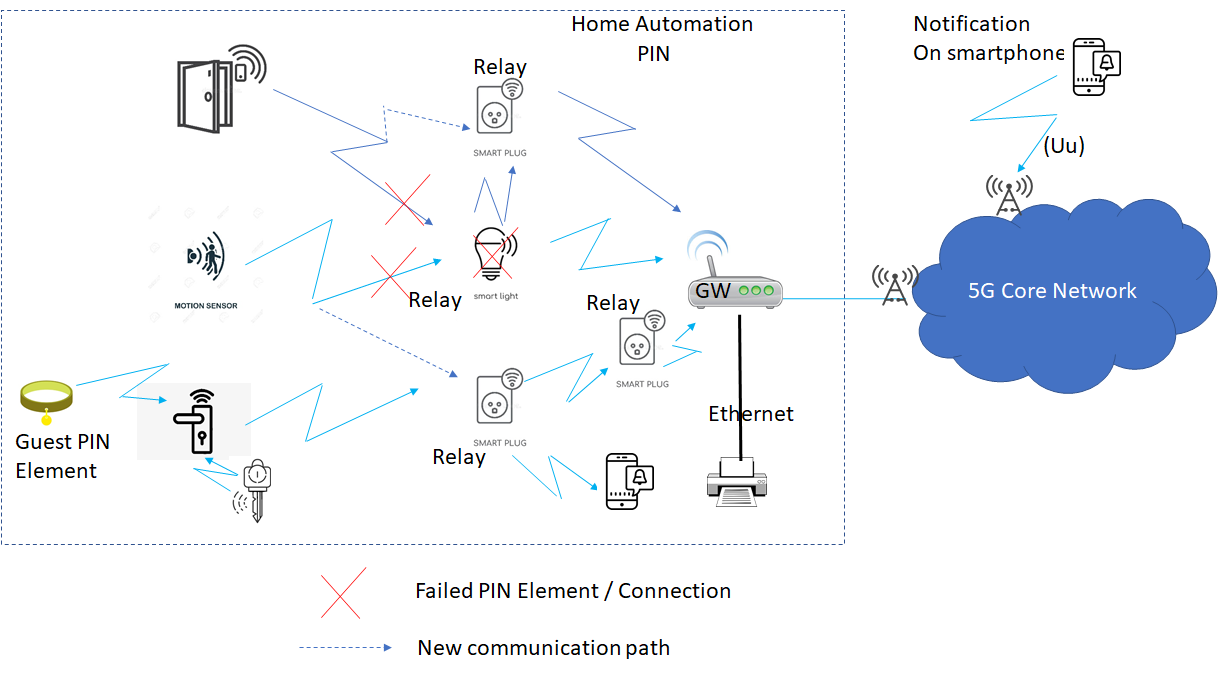
### 5.1.3 Service Flows

#### 5.1.3.1 General

Florence (PIN-User) has decided to build a home automation network (PIN) and has purchased a number of PIN 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 Elements). The instructions on the PIN Elements 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 Elements 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 Elements into the PIN Element with Management Capabilities. Checking her APP she sees one of the PIN Elements, a door sensors, is offline. Florences moves a PIN Element that acts as a relay, smart light bulb, per instructions she does a “Network configuration check” and then opens and closes the door and sees in real time the door sensor reports the action. A while later, at 10am, 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 as a notification has been provided on her smartphone and finds out her son turned the light switch off at 10am. She decides to install a smart light switch near the door sensor to prevent that issue of the door sensor going offline from occurring again.

Florence speaks to the voice assistant to give it a command to change the state of the light bulb, the light bulbs turns 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.

Figure 5.1.3.1-1 gives a pictorial view of the new configuration that Florence network can support where if a PIN Element fails communications can still take place via alterative route/path (see dotted blue lines). The diagram shows if the lightbulb is turned off communications can still take place via a power socket or light switch. It also shows Florence’s smartphone receiving a notification of the failures.

 Figure 5.1.3.1-1: light bulb failure (turned off)

When Florence installs a new PIN Element into the PIN the instructions indicate that the PIN Element with Management Capabilities has to be within 2m so that the 2 PIN Elements can successfully communicate. After that a PIN Element may use a PIN Element that extends the PIN network coverage to successfully communicate with the PIN Element with Management Capabilities.

#### 5.1.3.2. Onboarding

When Florence first setup her PIN she had one device that was designated as a gateway UE. 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 Element to be able to adds subsequent PIN Element to the PIN by scanning in a QR or bar code from the PIN Element.

NOTE 1: 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 Element 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 gateway UE being connected to the 5G network, but if the gateway UE is connected to the 5G network it will give her the option to:

a) allow her PIN to be more secure[[2]](#footnote-2). In this situation the PIN Element vendor provides the credentials that need to be downloaded into the PIN Element with Gateway capability; and

b) if a PIN Element, if it supports the capability, to have a better user experience e.g. security equipment, door locks have guaranteed real time operation. (e.g. using operator managed PIN direct connection).

NOTE 2: b) requires credentials to be managed by Florence’s service provider.

In both a) and b) the PIN can function (continue to operate) when the PIN Element with Gateway capability has connectivity to Florence’s service provider or does not have connectivity. In the case of b) and operator managed PIN direct connection is used the PIN element has to be in coverage of Florence’s service provider.

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 Element 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 Elements can interact with other PIN Elements 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 Requirements

[PR 5.1.5-1] The 5G system shall support the ability for a network operator or authorised 3rd party 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 can be up to 200ms [4] from the sending PIN Element to the receiving PIN Element (e.g. ask the voice assistant [sending PIN Element] to turn a light on [receiving PIN Element]). Other communication KPIs are shown in Table 5.1.5-1.

Table 5.1.5-1 – KPIs for communications within a home automation PIN

| Use case # | Characteristic parameter | | | Influence quantity | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Communication service availability: target value [%] | Communication service reliability: mean time between failures | End-to-end latency: maximum | Message size [byte] | Transfer interval | Survival time | PIN Element speed | # of PIN Elements in the service area | Service area (note 1) |
| US Home | 99.999 | TBD | 200ms[4] | TBD | TBD | TBD | stationary | [150][[3]](#footnote-3) | 214 sq m [11] |
| UK Home | 99.999 | TBD | 200ms[4] | TBD | TBD | TBD | stationary | 31 [12] + [12] NOTE 1 | 90 sq m [13] |
| NOTE 1 This assumes a UK house has medium rooms of: 3 bedrooms (2 double, 1 single), living room, kitchen, garage, 2 bathrooms, hallway and dining room. 31 sockets plus 12 lightbubs | | | | | | | | | |

NOTE: The definitions for the titles of each column can be found in 3GPP TS 22.104 [15].

[PR.5.1.5-3] The PIN shall support fault tolerant operations.

[PR.5.1.5-4] The 5G system shall support mechanisms to provision a PIN to use PIN direct connection in non-operator managed spectrum when it has no connectivity to the 5G system.

[PR.5.1.5-5] The 5G system shall support mechanisms for the PIN to collect charging information (e.g. timestamp for start and stop of communications, amount of data sent/received) regarding PIN Elements that use operator managed spectrum for PIN direct connections, and to report charging data to the 5G system.

[PR.5.1.5-6] The 5G system shall support a PIN Element using either non operator managed credentials (e.g. provided by a third party), or credentials that are managed by a service provider (e.g. see 3GPP TS 22.101 [3] clause 26A).

[PR.5.1.5-7] A PIN shall be able to still operate when no connectivity exists from a PIN Gateway to the 5CN and or internet.

NOTE 1: PIN Elements can only use non operator managed spectrum for communications and authentication mechanisms that do not require 5CN and or internet connectivity i.e. PIN Elements that are managed locally.

[PR.5.1.5-8] A PIN shall have a least one PIN Element with Management Capabilities.

[PR.5.1.5-9] The 5G network shall be able to provide backup of management data for PIN elements with management capability based on operator’s policy and local regulations.

[PR.5.1.5-10] A PIN Element shall efficiently support a PIN discovery mechanism where PIN Elements can discover, subject to access rights:

- status of other PIN Element (e.g. on/off);

- if the topology of the PIN has changed;

- capabilities of other PIN Elements (e.g. relay, PIN Element with management capabilities, PIN Element with gateway capabilities);

- PIN Element with gateway capability has external IP connectivity.

NOTE 2: external IP connectivity could be local break out or via the 5G core network.

- connection types support by other PIN Elements (e.g. operator managed, non operator managed); and/or;

- battery operated.

## 5.1A The lost dog

### 5.1A.1 Description

As more and more Personal IoT Networks are deployed there starts to become ubiquitous coverage provided by these networks. This allows for new service offerings to be offered to subscribers. One such offering is where PIN network owners, via user and or service provider authorisation can allow nomadic (guest) PIN Elements to use their PIN networks to reach a specific service in the cloud or in their own personal PIN. A small amount of bandwidth can be dedicated to this. One such offering can be found here [17].

In addition, the PIN network can contain multitude of devices, some using PIN direct connection’s that use operator managed spectrum and some that do not. Figure 5.1A.1-1 shows a possible guest PIN Element obtaining access via a PIN2. The user plane data is sent transparently (via a user plane pipe) from the guest PIN2 to a server in the cloud and then server communicates the user plane data to the smartphone (PIN Element) in PIN1.

NOTE 1: The contents of the user plane is outside the scope of 3GPP.

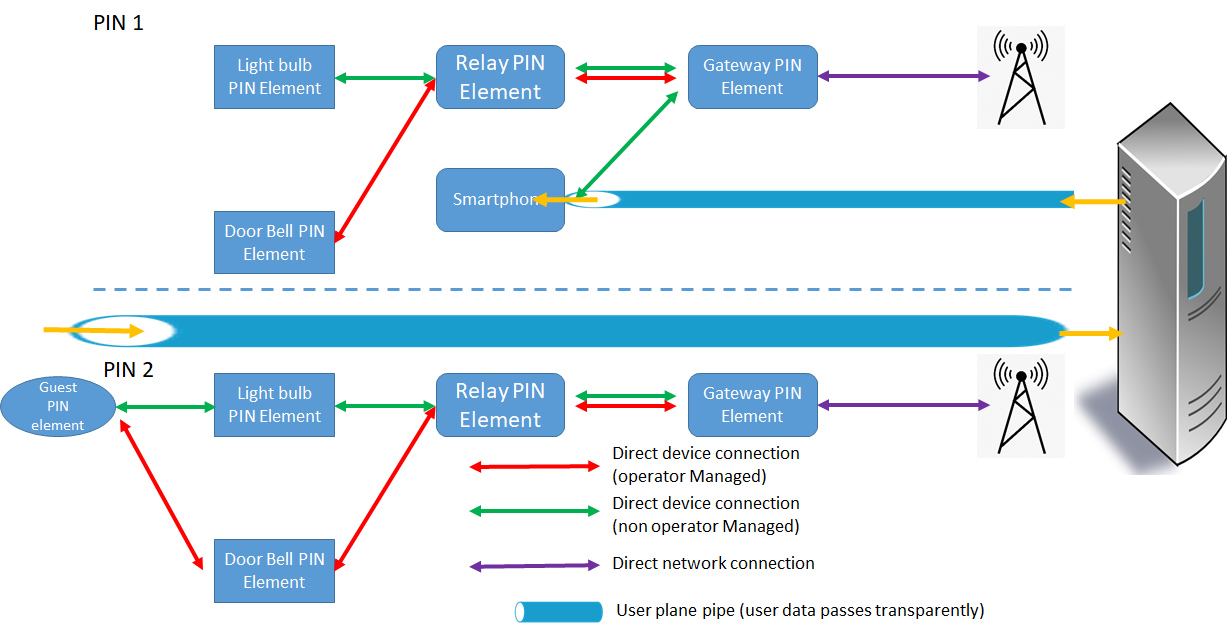


Figure 5.1A.1-1. Guest PIN Element accessing a PIN

### 5.1A.2 Pre-conditions

Florence (Usecase 5.1 as described in Clause 5.1) who lives at number 5 has installed her PIN. Florence has signed up for the guest PIN Element offering from her MNOa.

Houses Number 7 and 25 have installed PINs. They have been given a discount by their respective MNOs if they allow guest PIN Element usage of their PINs. Guest PIN Elements only get small amount of bandwidth from the PIN Network.

Houses 7 MNOc connection is having issues and has no connectivity to the 5G system.

Adrian has a wearables PIN and has been given the same respective discount by his MNOd. He has signed up as he is pet lover and wants lost dogs to be found.

Ellen has a PIN network and has a PIN Element (dog collar) on her dog Pilot to keep a track of him, it is configured to be a guest PIN Element. When the collar detects its outside of a geofence it will report its location (10 bytes in length [18][[4]](#footnote-4)) and Ellen will be alerted within 1 second. Ellen uses MNOc. According to the instructions that came with the dog collar it states it will report its location by using other PINs that have been deployed by people (e.g. doorbells, cameras, power sockets, watches etc) and that a person who deployed them has allowed them to use guest PINs. The owner of the dog collar does not have to ask every PIN owner to allow access.

MNOs provide a guarantee that guest PIN Elements will only consume X bytes a month.

### 5.1A.3 Service Flows

Pilot is a very smart and naughty dog, he loves to explore the neighbourhood and is an escape artist. Ellen has put a PIN Element (i.e low power tracking device) on his collar which when it is outside of a geofence area reports Pilots location. One day Pilot chases some squirrels and escapes from the backyard. As he roams the neighbourhood he passes houses with PINs, his collar reports its location via Florences network (light bulb PIN element in House 5) to a dog tracking service.

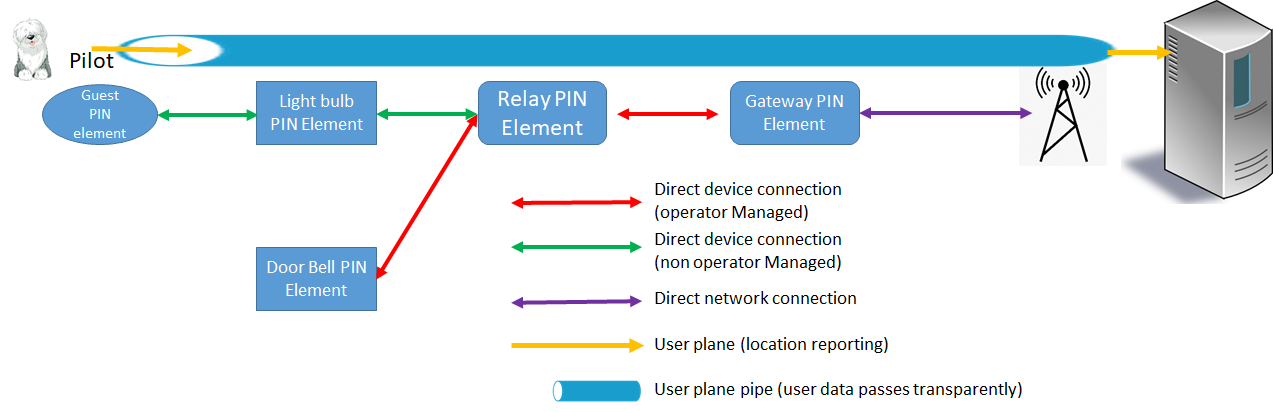


Figure 5.1A.3-1. Pilot accessing Florence’s PIN

House 7 is next, but as it has no connectivity the dog collar makes no report. He also passes Adrian who is in the park with his dog Pongo, Pilot says hello to Pongo and runs off. Adrian has a wearable PIN network and was listening to music so didn’t spot Pilot. As Pilot passed his collar reported its location via Adrians PIN.

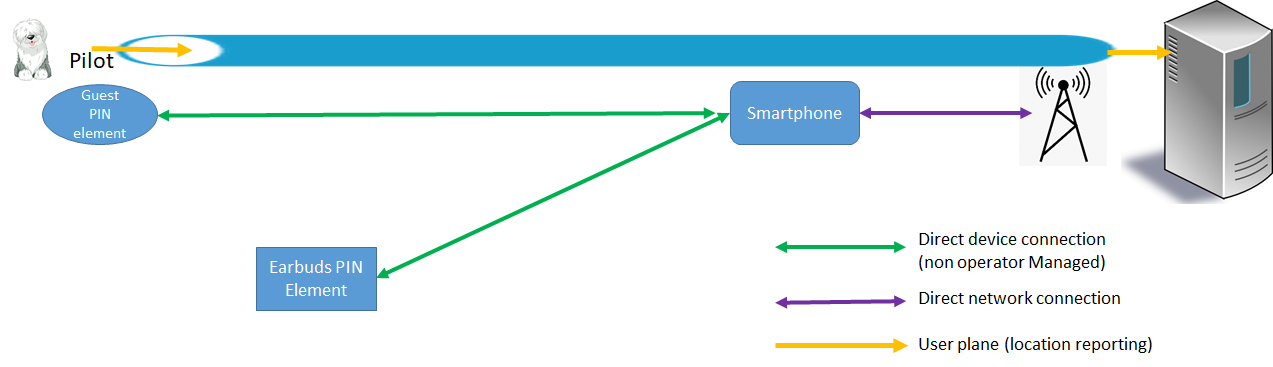


Figure 5.1A.3-2. Pilot accessing Adrians PIN.

Ellen is out grocery shopping and gets notifications on her phone, Pilot was seen at 1:10pm outside House 5 (House 7 also has a PIN but had no 5G connectivity) and later in the park near the dog park area. Ellen pays for her grocery’s and starts home. She sees on her smartphone Pilot has stopped at his favourite spot which happens to be by House 25 whose PIN Element door lock picked up pilots tracking device.

### 5.1A.4 Post-conditions

Ellen picks up naughty Pilot and takes him home. House 5, 25 and Adrian are not even aware that Pilot was by them. They are aware that some bandwidth was used but not by whom.

### 5.1A.5 Existing features partly or fully covering the use case functionality

3GPP 22.261 [2] clause 6.14 contains requirements regarding IoT devices accessing 5G system using a relay UE:

*An IoT device which is able to connect to a UE in direct device connection mode shall have a 3GPP subscription, if the IoT device needs to be identifiable by the core network (e.g. for IoT device management purposes or to use indirect network connection mode).*

### This also applies when using a non-3GPP direct device connection between the IoT device and the relay UE. In this use case the IoT device needs to be identifiable by the core network as the host UE and the guest PIN element have no relationship with each other, the host UE probably does not know the guest PIN element and is not responsible for its traffic. As such lawful interception and data retention etc. as well as charging should not be based on the identity of the host UE but of the guest PIN element.5.1A.6 Potential New Requirements needed to support the use case

None identified

## 5.2 Positioning with VR and AR

### 5.2.1 Description

It is more and more popular that immersive visual and game with the development of AR and VR. People are always looking for a realistic and interactive experience in the virtual and mixed world. Position tracking of UE devices (such as glasses, Handheld, and wearable devices) is crucial for the interactive experience.

### 5.2.2 Pre-conditions

The PIN Element (termed for glasses, smartphone, etc. wearable devices, power point, light bulb etc.) can send out signals that can enable other PIN Elements to measure and conduct positioning based on the measurements from the signals. The PIN user is aware that they need to position a number of PIN Elements in their room / house so that their PIN Elements that participate in AR/VR games can provide precise position into AR/VR games.

The PIN Devices use PIN direct connections to communicate with each other.

There is an immersive game called NEXGalaxy. In the game, the BOAT(s) are chasing and competing for limited resources on different planets in the universe. Each player has control of the speed and direction of a BOAT with a smartphone (PIN Element). Each player is also viewing the planet with the glasses (PIN Element) they are wearing. The BOAT can also be moved laterally if the controller/player walks or jumps left and right. Depending where the player stands in the room dictates where the player starts in the game e.g. which lane etc. When the game console was setup that hosts the NEXGalaxy game the user (PIN User) had to enter the game consoles position in the room, including room rough dimensions and a rough map of major obstacles e.g. sofa, dining table etc. The map is such that participants in the game are kept at least half a bodies distance from obstacles. This allows the game console to allow a person to move around in the room without hitting obstacles there as the game requires a lot of movement, the movement being reflected as actions in the game. E.g. in NEXGalaxy there is volcano that you can look around, the game console can setup the AR such as a dining table could be the volcano and as person walks around the dining able they walk around the volcano. Players also jump to perform actions in the game, however as a person jumps they change their position in the room and the game display has to adapt to ensure the person does not hit a table, sofa, chair etc.

Friends Yuan and Xun each other their own smartphone (PIN Element) and a smartring (PIN Element). Yuan owns a pair of VR glasses (PIN Element). Each has configured a personal PIN:

- Yuan’s PIN consists of the following PIN Elements: her smartphone, smartring, 2 VR glasses, a number of smart home automation devices e.g. power socket, light bulbs;

- Xun’s PIN consists of the following PIN Elements: her smartphone and smartring.

Each PIN Element has at least an accelerometer in it.

Yuan has subscribed to a service from her service provider to provide an operator managed games service that among other things provides the ability to provide accurate absolute positioning. This operator managed game services uses the operator direct device connections capability using the operators managed spectrum.

### 5.2.3 Service Flows

Yuan and her friend Xun want to play the immersive game NEXGalaxy in Yuan’s home. They want to enjoy virtual scenarios and real interaction in Yuan home through some PIN Elements (e.g. glasses, smartphone, and wearable devices). Yuan scans a QR code on Xun’s smartphone (PIN Element) screen so that Yuan can allow Xun to play the game via Yuan smartphone (PIN Element). Yuan also lets Xun borrow one of her VR glasses (PIN Element). Xun configures her smartphone (PIN Element) to communicate with the borrowed set of VR glasses (PIN Element).

- Yuan and Xun put on some VR glasses (PIN Element) and hold their smartphone (PIN Element) and began the games. They each control a BOAT. They start the BOAT using the smartphone (PIN Element) at the same time from the Base in MARs and compete to see who get to the Volcano first.

- Yuan starts more quickly by controlling the BOAT using the smartphone (PIN Element).

- Xun launches a missile targeting Yuan by using the smartphone (PIN Element) to aim at Yuan.

- Yuan jumps right and left to avoid the missile.

- During the time when Yuan tries to avoid the missile, Xun accelerates her BOAT through the smartphone (PIN Element) and begins to lead in the race.

- Xun wins the game. She walks off the plane and turns her head around to check the views around the volcano. It’s really beautiful.

Yuan and Xun feel excited about the games. They continue to play the game about an hour.

### 5.2.4 Post-conditions

Yuan and Xun take off their glasses (PIN Element) and put their smartphone (PIN Element) down. They are discussing the details in the game and check the details through replay on their smartphones.

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

None identified.

### 5.2.6 Potential New Requirements needed to support the use case

[PR 5.2.6-1] The 5G system shall support that a PIN Element may be a member of more than one PIN.

[PR 5.2.6-2] The 5G system shall support a PIN Element being added or removed from a PIN by an authorised 3rd party.

[PR 5.2.6-3] The 5G system shall enable PIN direct connections between PIN Elements in a PIN to use licensed spectrum (under the control of a MNO) or between PIN Elements to use unlicensed spectrum (may be under the control of the MNO, or not).

[PR 5.2.6-4] The 5G system shall be able to support positioning for PIN Elements in a PIN.

## 5.3 Media share within PINs Use case

### 5.3.1 Description

Nowadays a person has many electronic devices, such as smart phone, TV, earbuds, speaker, watch, and AR glasses (known as PIN Elements). Ideally the user should be able to choose the device he/she wants to watch the video/listen to the audio among all the devices the user has, with simple operation, without interruption the media being watched.

The media transmitted by a PIN Element could voice, video, Game audio/video and other type of data traffic. The media could be generated locally in the PIN network or from application server. Media share within PINs mean:

- the owner of PIN could choose any device to play the media; or

- the owner of PIN could switch from one PIN Element to anther PIN Element and the media continue to play during the switch between the PIN Elements.

### 5.3.2 Pre-conditions

The User has a smartphone (PIN Element) and at least one of smart earbuds, AR glasses, watch and TV, baby monitor speaker (PIN Elements). The first 3 (smart earbuds, AR glasses, watch) are collectively known as wearables. The collection of all 6 is known as a Personal IoT Network (PIN). All the PIN Elements communicate wirelessly using PIN direct connections.

The user uses the PIN Elements for entertainment, for example, listening to music, watching videos and having WeChat video and phone calls. The earbuds will play notifications, sound and the AR glasses will display video images and notifications. The speaker will play sound.

The user uses the PIN Element to check the real-time monitoring recording (baby camera) of the baby or the house when in or outside of house.

Media (video, audio, voice and etc.) originates from within the PIN e.g. music from smartphone, video and audio from the baby monitor.

### 5.3.3 Service Flows

Whenever the user listens to music, watches movie and has WeChat video and phone calls, the media(audio/video) can be shared among all the devices belonging to the same PIN, and therefore the media can be easily switched to other PIN Elements in the same PIN without interruption to the user entertainment.

**Service flow 1\_watch a movie:**

1. The user starts to watch a movie on the smart phone. The movie is coming from a streaming platform.

2. The user finds this movie very interesting and decide to watch the movie using AR glasses for 3D audio-visual enjoyment which uses PIN direct connections to transfer the media from the smartphone to AR glasses.

3. The user wears the AR glasses and choose the movie that was being watched on the smart phone.

4. The AR glass continue to play the movie from the part that was paused on the smart phone.

5. The user starts enjoying the movie on the AR glass with better 3D audio-visual enjoyment.

**Service flow 2\_listening to an audio book or music**

1. The User is doing housework with the speaker playing some audio book or music that are stored on the user’s smartphone. The connection from the smartphone to the speaker is using PIN direct connection.

2. The user decides to go running after finishing the house work.

3. The User wears the earbuds and the audio seamlessly switched from the speaker to the earbuds that communication with the smartphone using PIN direct connection.

4. The user goes out for running wearing the earbuds and watch, without carrying the smart phone.

5. The audio continues to play while the user runs outside using the cellular network to communicate with the watch which subsequently uses direct device connection to communicate with the earbuds.

**Service flow 3\_ baby monitor**

1. The user has bought a baby monitor (PIN Element) in their house, the instructions indicate that other PIN Elements can be used to extend the range of the baby monitor and as well if the purchaser wants they can use multiple PIN devices to make the baby monitor solution more resilient.

2. The baby is put for a daytime nap and the user needs to do some housework. The video from the camera that is in the house is sent to his smartwatch via a PIN direct connection so he can keep an eye on the baby.

3. In a few rooms of the house he has a large TV and as he goes into a room with a TV the video then appears on the TV from the baby monitor using PIN direct connections to the TV so the user can get on with what he needs to do but can keep an eye on the baby, this is more convenient than looking at a small image on the smartwatch.

4. The TV/smartwatch detects when the user cannot see the TV and stops displaying the video stream.

5. The user enters another room with a large TV and the same thing happens, again PIN direct connection is used from the video camera to the TV.

6. He then moves to the kitchen. As he is cleaning in the kitchen the baby wakes up and he hears the baby crying on the voice assistant that is in the kitchen. The voice is from the video camera and uses PIN direct connections to communicate with the voice assistant.

7. The user uses the PIN Element to check the real-time monitoring recording of the baby when outside of house.

**Service flow 4\_Over the top application call**

1. when the user is running outside wearing his watch, that uses direct network connection, he receives an over the top application call from his friend.

2, The user starts to talking to his friend on the over the top application using his watch and his earbud while walking back home.

3. When the user arrives home, he got a notification that the battery of his watch is low, so he picks up his smartphone that uses a direct network connection and continues to talk to his friend on the over the top application using his smartphone and earbuds.

4. During his over the top application call with his friend, his friend experiences no interruption at all.

NOTE: In service flow 4 there is only one PIN however it has 2 entry points from the operator’s network, the watch and the smartphone.

### 5.3.4 Post-conditions

The users can freely switch the video and/or audio between PIN Elements used and enjoy the same media (audio/video/voice calls) without interruption.

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

3GPP TS 22.228 [8] specifies the IP Multimedia (IM) Core Network (CN) subsystem inter-UE transfer (IUT), which provides the capability of continuing ongoing communication sessions with multiple media across different user equipment’s (UEs) under the control of the same or different subscribers, and as part of Service Continuity (SC).

3GPP TS 22.228 [8] is not applicable to non-IMS session inter-UE transfer when using direct device connections.

3GPP TS 22.261 [2] clause 6.2.3 has following requirements

- The 5G system shall support service continuity for a remote UE, when the remote UE changes from a direct network connection to an indirect network connection and vice-versa.

- The 5G system shall support service continuity for a remote UE, when the remote UE changes from one relay UE to another and both relay UEs use 3GPP access to the 5G core network.

3GPP TS 22.261 [2] clause 6.9.2.1 has the following requirements:

The 5G system shall support the relaying of traffic between a remote UE and a gNB using one or more relay UEs.

The 5G system shall be able to support a UE using simultaneous indirect and direct network connection mode.

3GPP TS 22.278 [5] defines ProSe Group Communication:

**ProSe Group Communication:** a one-to-many ProSe Communication, between more than two UEs in proximity, by means of a common ProSe Communication path established between the UEs.

In 3GPP TS 22.278 [5] clause 7A.1 defines precisely the means and constraints by which ProSe Group Communication can be enabled and used.

### 5.3.6 Potential New Requirements needed to support the use case

[PR 5.3.6-1] For intra-PIN communications, a PIN Element shall be able to transmit media to one or more PIN Element at the same time.

[PR 5.3.6-2] A PIN Element shall support service continuity when a PIN Element changes the communication path from one PIN Element to another PIN Element. The communication path between PIN devices may include both 3GPP and non-3GPP access.

[PR 5.3.6-3] For a PIN it shall be possible to have more than one PIN Element with Gateway Capability.

Editors Note: SA3 need to be consulted on the security aspects of having more than one PIN Element with Gateway Capability in the PIN.

## 5.4 Switching between non-3GPP RAT and 3GPP RAT direct device connections Use case

### 5.4.1 Description

There are lots of cases that Smart glasses are paired with a smartphone using non 3GPP RAT for transmitting video information from the smartphone to smart glasses. However, non 3GPP RATs are based on unlicensed frequency. In some areas, if lots of people use unlicensed frequency, the quality of service will be bad. If and when the quality of service goes down the service could be switched to a 3GPP RAT (direct communications) autonomously and the user could have a better experience. In addition, the opposite could be true in that the direct communications could be congested, and therefore it makes sense that both non 3GPP RAT and direct communications could be used together.

### 5.4.2 Pre-conditions

Lihua has one smartphone and one smart glass. The Smartphone (PIN Element) can connect with the Smart glasses (PIN Element) using non 3GPP RAT direct device connections capability. This is Lihua’s Personal IoT Network (PIN).

Lihua has also subscribed to her service provider for an operator managed video service, therefore, the Smartphone (PIN Element) can also connect with the Smart glassed (PIN Element) using the operator direct device connections capability using operators managed spectrum. The service provider bills based on data consumption, time, or the operator managed resources used for the service data transmission, e.g. operators managed spectrum. The Smart glasses (PIN Element) can determine if non 3GPP RAT and or the operator managed direct device connections capabilities are congested or not. If operator managed direct device connection service is not available e.g. out of 3GPP coverage the service will not be used by a PIN Element and non 3GPP RAT direct device connection can be used.

The Smart glass (PIN Element) can transmit the video service via both the WLAN and the operator managed direct device connections capability simultaneously. The smartphone is allowed to select to transmit over non 3GPP RAT direct device connection or the non-operator managed spectrum based on some criteria, which are provided by lihua or the operator. The smartphone (PIN Element) allows Lihua to set up a set of parameters to control the video quality when her operator managed video service will be used so that she can control the usage of her operator managed direct device connections provided service.

If requested by the operator, the Smartphone (PIN Element) collects and reports to the operator network the statistics information of the non 3GPP RAT direct device connection, such as the data volume transmitted over non 3GPP RAT direct device connection or the non-operator managed spectrum, if 3GPP authentication was used, service discovery was used.

### 5.4.3 Service Flows

Lihua has one smartphone (PIN Element) and one smart glasses (PIN device). The Smartphone (PIN Element) connects with the Smart glasses (PIN Element) using non 3GPP RAT direct device connection for transmitting video data from the smartphone (PIN Element) to the smart glasses (PIN Element). After work Lihua take the subway back home, she lives in Vienna that has great continuous coverage in the subway system. Lihua watches the video on her smart glasses (PIN Element). The video is being played from her smartphone (PIN Element). When Lihua enters the subway station where there are lots of people, the smart glasses (PIN Element) detects that the quality of non 3GPP RAT direct device connections is bad and the smart glasses (PIN Element) requests the smart phone (PIN Element) to switch all or some of the video packets to operator managed direct device connection service. Lihua may get a notification that this happens however it’s the start of the month and she has turned off notifications. Based on some criteria, which are provided by lihua or the operator, the smart phone (PIN Element) requests from the network for some operator managed direct device connections resource to stream the video from the smartphone (PIN Element) to smart glasses (PIN Element). While the video service is transmitted from the smart phone (PIN Element) to smart glasses (PIN Element) using the operator managed direct device connection resource and when requested by the operator, the smart phone gathers the information needed for charging and reported to the operator network. The information needed for charging includes the data transmitted for the video service over the operator managed direct device connection between the PIN Element, time, the operator managed resources used for the service data transmission, e.g. operators managed spectrum and etc.

As Lihua rides the subway, more and more passengers get on. These passengers have also subscribed to the same video service. After some time, the network has limited operator managed direct device connections service resources to give Lihua. However, the smart glasses (PIN Element) finds that some non 3GPP RAT direct device connections resources can be used. The smart phone then aggregates non 3GPP RAT with operator managed direct device connection services Lihua can receive uninterrupted viewing experience.

If requested by the operator, the Smartphone (PIN Element) collects and reports to the operator network the statistics information of the non 3GPP RAT direct device connection, such as the data volume transmitted over non 3GPP RAT direct device connection or the non-operator managed spectrum if 3GPP authentication was used, service discovery was used.

### 5.4.4 Post-conditions

Lihua watches the movie and notices no degradation in video quality moving into and out of the subway as other people around have issues with their connectivity.

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

3GPP TS 22.261 [2] "The 5G system shall be able to support a UE using simultaneous indirect and direct network connection mode" indicates that a UE can transmit simultaneously however direct network mode is between a UE and the network. The use case in sub-clause 5.4.3 has no user plane traffic (i.e. movie) going to the network.

3GPP TS 22.278 [5] "Subject to operator policy and user consent the EPC and a ProSe-enabled UE shall be capable of negotiating the move of a traffic flow between the EPC Path and the ProSe-assisted WLAN direct path." Indicates that a UE can move traffic between an EPC Path and ProSe WLAN direct path however the use case in sub-clause 5.4.3 has no user plane traffic (i.e. movie) going to the network

3GPP TS 22.278 [5] "Both the HPLMN and VPLMN operators shall be able to charge for ProSe-assisted WLAN direct communications. " however these requirements are written in the context of the network being involved and user plane traffic going to the network.

### 5.4.6 Potential New Requirements needed to support the use case

[PR 5.4.6-1] The PIN Element can act upon user and operator preferences to aggregate, switch or split the service between non-3GPP RAT and operator managed PIN direct connection services.

[PR 5.4.6-2] When operator managed PIN direct connections are used for PIN UE Element communications the 5G System shall be able to collect charging data, including data transmitted over the operator managed PIN direct connections between the PIN Elements, time, the operator managed resources used for the data transmission, e.g. operators managed spectrum and etc.

[PR 5.4.6-3] When PIN UE Element uses unlicensed spectrum for direct device connections for intra PIN UE device communications the 5G System may, subject to local/regional regulations and user consent, collect statistics data, including if 3GPP authentication was used.

## 5.5 Use case: UE accessing Services provided by PIN Elements behind 5G enabled gateway(s)

### 5.5.1 Description

There are more and more IoT devices or none-3GPP devices, e.g. media server, printer, smart thermostat/sprinkler/blinds, NAS server, smart plug, smart watch, smart pet collar, earbuds, VR goggle headset, smart garage door, etc., that can provide services for users at home or out of home in the home settings. These devices are usually behind a wireless gateway. In recent years, there are some security risks found in such settings due to port forwarding and unsecure connectivity provided by the wireless gateway for in home devices.

When considering the gateway with 5G capability for accessing 5G services, , it is important to enable the support of the secure connectivity for allowing authorized users from anywhere in the world to access authorized services provided by these IoT devices or none-3GPP devices in terms of user authentication and authorization.

These IoT devices or non-3GPP devices acting as a PIN Elements can be smart plug, smart watch, smart pet collar, earbuds, VR goggle headset, etc. that usually are connected to the UE as a PIN Element with Gateway Capability via non-3GPP access, e.g. WLAN, Bluetooth®. When the UE moves, the PIN moves with the UE and its associated PIN Elements. These PIN Elements authorized to communicate with each other are regarded in a Personal IoT Network (PIN). There are other IoT devices, or non-3GPP devices usually stationary connected to the eRG using non-3GPP access (WLAN, wireline), e.g. media server, printer, smart thermostat, smart sprinkler, smart blinds, smart garage, etc. These IoT devices or non-3GPP devices authorized to communicate with each other directly or via the eRG are regarded in a Customer Premises Network (CPN).

Editor's Note: this use case assumes that evolved residential gateway (eRG) defined in TR 22.858 [6] can operate as a PIN Element with Gateway Capability, which needs further clarification between two studies. For example, in the home or office settings, the PIN Element (non-3GPP device) is stationary installed and can be media server, printer, smart thermostat, smart sprinkler, smart blinds, smart garage door, etc., which can connect to the eRG using non-3GPP access, e.g. WLAN, wireline.

Figure 5.5.1-1 shows the scenarios of the 5G network enabling connectivity service support for the UE using direct network connection (case a) or direct device connection or PIN direct connection (case b and case c) to access services provided by PIN Element. Each PIN Element may provide one or more services. For example, the PIN Element is a smart watch, earbuds, VR goggles, media server, smart TV, smart video doorbell, etc., which provide one media service. For another example, the PIN Element is a NAS server which can provide multiple services, e.g. media service, web server service, live security cams services, etc.



Figure 5.5.1-1: 5G network support for a User/UE accessing services provided by PIN Element (dash line is direct device connection or PIN direct connection; solid line is direct network connection)

In Figure 5.5.1-1, a user using an authorized UE, e.g. smartphone or tablet, accesses the service A provided by an PIN Element which has connection with PIN Element with Gateway Capability via a non-3GPP access technologies, e.g. WLAN, Bluetooth®, etc.

Case (a): the user/UE is out of Home and uses authorised service A provided by a PIN Element behind a PIN Element with Gateway Capability which relays traffic to and from 5G network. The PIN Element with Gateway Capability and the PIN Element connects to each other using direct device connection or PIN direct connection while the PIN Element with Gateway Capability connects to the 5G network using direct network connection.

Case (b): the user/UE operating as a PIN Element is at home and uses authorised service A on the other PIN Element via PIN Element with Gateway Capability which supports relay communication between two PIN Elements. The UE and the PIN Element connect to PIN Element with Gateway Capability using direct device connection or PIN direct connections. One or more PIN Elements can connect to the PIN Element with Gateway Capability.

Case (c): the user/UE operating as a PIN Element is at home and uses authorised service A directly provided by the PIN Element using direct device connection or PIN direct connection. If connecting to 5G network is required by the PIN Element, the UE can operate as a PIN Element with Gateway Capability to relay traffic to/from the PIN Element.

To avoid the potential security/privacy risks that invade the PIN Elements and services, it is important that the 5G network can enable supports of secure access to the PIN Elements and their services for authenticated and authorized users. According to 3GPP TS 22.101 [3] clause 26a, an "User" to be identified could be

- an individual human user, using a UE with a certain subscription, or

- an application running on or connecting via a UE, or

- a device ("thing") behind a gateway UE.

In the context of PIN (personal IoT network), a "User" includes a service ("application”) running on or connected via a PIN Element behind a PIN Element with Gateway Capability.

The following service aspects for IoT device and non-3GPP device as PIN Element connected to the 5G network via a PIN Element with Gateway Capability, needs to be considered:

- User Identity and user authentication;

1. User Identity of PIN Element or application running on PIN Element;

2. The authentication of User Identity or application running on the PIN Element;

- Access to PIN Element or its application running on the PIN Element;

- User Profiles and User Identifiers for PIN Element or its applications provided by an PIN Element;

- UE policies in the home settings.

### 5.5.2 Pre-conditions

The Incruedible family adopts civilian identities and lives at suburbs for a normal life to hide their superheroes identities. To ensure secure communication for the Incruedible family accessing services of PIN Elements from anywhere in the world, Mr. Incruedible sets up many PIN Elements and subscribes to a reliable network operator’s services, which can act as User Identity provider and provide secure access to his PIN Elements and the applications running on or connected to the PIN Element behind the PIN Element with Gateway Capability, for all UEs of his family, including smartphones, tablets.

### 5.5.3 Service Flows

**Step1: [Users configuration]**

Mr. Incruedible, signs in his account at operator’s network that provides 5G connectivity services for all UEs of his family. In his account, there are two listed subscriptions with gateway capabilities, including one smartphone , i.e. a UE as PIN Element with Gateway Capability, and one eRG. In Mr. Incruedible’s account, he can create Users with User Identities for family members, PIN Elements, and services provided by PIN Elements.

Further, for each service of the PIN Element behind a PIN Element with Gateway Capability, Mr. Incruedible configures User Profiles, e.g. via scanning the QR code of the PIN Element to get some information and editing details manually. For each service identified by a User Identity, it can have one or more User Profile(s) and each User Profile contains the following information:

- User Identifier

- Specific service settings and parameters, e.g. active/inactive time, number of accesses, etc.

- Authentication/authorization policy and access restriction policy required for the service, which are going to be used to authenticate/authorize a User for accessing to the PIN Element or application running on the PIN Element.

- Credential information, e.g. password for the authorized service, security keys for encryption/decryption, and hash algorithm for message digital signing, etc.

For an authorized human user(s), its User Profile can indicate the authorized service identified by User Identity and allowed User Identifiers.

**Step2: [Registration of PIN Element and Update of User Profiles for services provided by the PIN Element]**

(2a): When an PIN Element is turned on, the PIN Element with Gateway Capability discovers and connects to the PIN Device at the first time, the PIN Element with gateway Capability determines if the PIN Element is an authorized User identified by a User Identity indicated in its UE configuration.

(2b): The serving network of the PIN Element with gateway Capability authenticates User Identity of the PIN Element based on its credentials, and then updates User Profiles of the services provided by the PIN Element. In return, the network responds the PIN Element with gateway Capability with the authentication result and updated User Profiles of the registered services.

(2c): The serving network of the PIN Element with gateway Capability further provides updated User Profiles of the services to 5G subscriber’s HPLMN. The HPLMN of PIN Element with gateway Capability updates its stored User Profiles of all impacted Users.

(2d): Based on serving network’s policies, the serving network can update User Profiles of impacted Users and UE configuration towards PIN Element with gateway Capability.

**Step3: [User/UE at home or out of home accessing services provided by PIN devices]**

Violeta, Mr. Incruedible’s daughter as an authorized user (User) of the service provided by a PIN Element, would like to use the authorized UE to access a registered application-A of a PIN Element behind a PIN Element with gateway Capability. For example, the PIN Element is a smart garage door and Violeta would like to request the smart home application-A on the PIN Element to open the garage door for the delivery crew to put the package inside the garage. The communication method that connects her UE and the PIN Element is different based on the location of her UE as follows:

- Case (a): When Violeta (User) using authorized UE is out of home, the 5G network connects the UE to the PIN Element behind the PIN Element with gateway Capability.

- Case (b): When Violeta (User) using authorized UE is at home, the PIN Element with gateway Capability discovers and connects the UE acting as an PIN Element and using PIN direct connection or direct device connection based on stored UE policies or user preferences.

- Case (c): When Violet (User) using authorized UE is at home, the UE acting as a gateway UE discovers and connects with PIN Device directly via a non-3GPP access technologies, e.g. Bluetooth, WiFi, or via 3GPP direct communication, instead of via indirect communication over 5RG, based on stored UE policies of the UE or user preferences.

(3b): Based on stored User Profiles of the PIN Element with authorised Users, the PIN Element with gateway Capability can determine whether to accept access request of the PIN Element from the User/UE.

(3c): The PIN Element with gateway Capability can further perform user authentication of the application-A based on the security polices and credentials in stored User Profiles of the application-A. If the application-A is configured to apply user authentication by the 5G system, the PIN Element with Gateway Capability requests user authentication for the application-A by the 5G system.

(3d): The PIN Element with gateway Capability forwards the service access request to the PIN Element only if the user authentication is successful. Otherwise, the PIN Element with gateway Capability rejects the request for service access.

(3e): The PIN Element with gateway Capabilitystarts to forward the traffic to/from the PIN Elements.

**Step4: [UE policies in the home settings]**

When the authorized User/UE moves from out of home, i.e. case (a), to in home, i.e. case (b) or case (c), the User can manually determine how the used UE adopts case(a)/case (b)/case(c), or UE can automatically adapt to case(a)/ case(b)/case (c) based on the UE policies, including the following information provisioned by the 5G network:

- one or more operation modes (e.g. PIN Element, UE, PIN Element with gateway Capability);

- communication methods (e.g. direction network connection, direct device connection, PIN direct connection);

- location information.

### 5.5.4 Post-conditions

The Incruedible family can safely live with hidden superheroes identities by securely accessing application of the PIN Elements from anywhere in the world without compromising the security of the PIN Elements/services at home.

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

Referring to 3GPP TS 22.101 [3] clause 26a, the user to be identified could be an individual human user, using a UE with a certain subscription, or an application running on or connecting via a UE, or a device (“thing”) behind a gateway UE. The following service requirements have been supported:

- The 3GPP network shall be able to provide a User Identifier for a non-3GPP device that is connected to the network via a UE that acts as a gateway.

- The 3GPP network shall support to perform authentication of a User Identity used by devices that are connected via a UE that acts as a gateway.

- The User Identifier may be provided by some entity within the operator’s network or by a 3rd party.

- The 3GPP system shall be able to take User Identity specific service settings and parameters into account when delivering a service.

NOTE: The requirement applies to 3GPP services and non-3GPP services that are accessed via the 3GPP System

- The 3GPP system shall be able to store and update a User Profile for a user.

- The 3GPP System shall support to authenticate a User Identity to a service with a User Identifier.

- When a user requests to access a service, the 3GPP System shall support authentication of the User Identity with a User Identifier towards the service if the level of confidence for the correct association of a User Identity with a User Identifier complies to specified policies of the service.

- A service shall be able to request the 3GPP network to only authenticate users to the service for which the association of the user with a User Identifier has been established according to specified authentication policies of the service.

- Subject to operator policy, the 3GPP system shall be able to update User Profile related to a User Identifier, according to the information shared by a trusted 3rd party.

- The User Profile may include one or more pieces of the following information:

- additional User Identifiers of the user's User Identities and potentially linked 3GPP subscriptions,

- used UEs (identified by their subscription and device identifiers),

- capabilities the used UEs support for authentication,

- information regarding authentication policies required by different services and slices to authenticate a user for access to these services or slices.

- User Identity specific service settings and parameters.   
Those shall include network parameters (e.g. QoS parameters), IMS service (e.g. MMTEL supplementary services) and operator deployed service chain settings.

- User Identity specific network resources (e.g., network slice).

The following service requirement in TS 22.101 clause 26a provide the principle for user centric identifiers and authentication by the 3GPP system:

- The 3GPP System shall support operators to act as User Identity provider and to authenticate users for accessing operator and non-operator deployed (i.e. external non-3GPP) services.

This use case and requirements consider that the application running on the PIN Element is a non-operator deployed (i.e. external non-3GPP) services behind a PIN Element with Gateway Capability in a PIN.

### 5.5.6 Potential New Requirements needed to support the use case

[PR-5.5.6-1]: The 5G system shall support secure mechanisms for a PIN Element using direct PIN connection or via PIN Element with Gateway Capability to access and communicate with another PIN Element for a PIN.

Editor's Note: evolved residential gateway (eRG) defined in 3GPP TR 22.858 [6] is assuming with PIN element gateway capability which needs further clarification in both studies.

[PR-5.5.6-2]: A gateway UE (or eRG) shall be able to store and update a User Profile associated to PIN Device or an application running on or connected to a PIN Device behind the gateway UE and the User Profile shall include one or more pieces of the following information related to this application:

- User Identifier

- Specific service settings and parameters, e.g. active/inactive time, number of accesses, etc.

- Authentication/authorization policy and access restriction policy required for the application, which are going to be used to authenticate/authorize a user for accessing to the application of the PIN Device.

- Credential information, e.g. password for the authorized service, security keys for encryption/decryption, and hash algorithm for message digital signing, etc.

Editor’s note: the service requirements need to be revisited in the next meeting.

## 5.6 UE accessing PIN applications hosted by a PIN Element with Gateway Capability

### 5.6.1 Description

PIN elements (e.g. media server, printer, smart thermostat/sprinkler/blinds, smart lightning system, NAS server, etc.) can be located behind a PIN Element with Gateway Capability (e.g., a residential gateway with PIN capability, or a UE with gateway PIN capability). This PIN Element with Gateway Capability can host, or locally be connected to, significant compute and storage resources. , which can host an Application Server. An application on an Application Server can be either in the MNO domain (i.e. a trusted application) or external to the MNO domain (i.e. an authorized third-party application).

An AS can be useful to process sensitive data locally. Data generated by some PIN elements can be sensitive, it is therefore important to limit the scope of its dissemination (e.g. temperature and light readings can be used to know if there is someone at home). The AS can also be useful to perform latency sensitive processing. For games and office applications it can be beneficial to render a latency sensitive application locally. The AS can be accessed by local users located in the PIN network, or by remote users connected through the 5G network.

The AS can be hosted on a locally connected hardware hosting platform (e.g., a game console, an application server), and/or be embedded in a PIN Element with Gateway Capability (e.g., leveraging virtualization technology to host AS on the PIN element). While an AS can be a standalone service, it can also be an on-site extension of an in-network service hosted on a hosting environment such as an edge computing platform. In this case, the service operator (e.g., a MEC server operator), can influence discovering/authorizing/orchestrating an AS. The AS can be under the control of a 5G network operator, a customer or an authorized third party.



Figure 5.6.1-1. UE Accessing a PIN application hosted by a PIN Element with Gateway Capability

Case (a): the user/UE1 is at home and uses a client application that connects to an AS deployed at home.

Case (b): the user/UE2 is out of home and uses a client application that connects to an AS deployed at home (on the PIN Element with Gateway Capability or on other hardware at home). UE2 is connected to the 5G network, e.g., it may be in another PIN.

Service aspects:

1) Deployment of an AS on a hosting platform on, or locally attached to, a PIN Element with a Gateway Capability hosted Service Hosting Environment and hosted on the applications by service provider.

2) Access to AS hosted in PIN, by UE2 outside of home.

3) Additional aspects are already covered in 3GPP TR 22.858 [6], clause 5.4 and clause 5.5. Therefore no specific new routing support is needed between PIN element/UE1 and AS:

a) Access to AS in PIN by UE1 or PIN device from inside home.

b) Access to services offered by PIN elements or UE1 from AS in PIN.

### 5.6.2 Pre-conditions

User deploys PIN elements behind a PIN Element with Gateway Capability and subscribes with a service provider for AS. This subscription can be directly with the service provider(s), or through a 5G network operator.

### 5.6.3 Service Flows

1) Setup:

a) Hosting environment is installed on PIN Element with Gateway Capability or other PIN element with compute/storage capability (by service provider, 5G network operator or User). User requests some compute/storage resources (in PIN Element with Gateway Capability or other PIN element with compute/storage capability) to be reserved for usage by the hosting environment

b) Service provider can provide and configure an AAA server to control access to AS hosted in PIN.

c) AS is enabled on hosting environment (by service provider, 5G network operator or User).

2) Using an AS:

a) User installs client applications on UE, e.g. a client application that configures temperature at home based on time or day or other triggers.

b) Service provider provisions corresponding serving AS in hosting environment in PIN.

c) Client application on UE connects through 5G network to serving AS in PIN, after authorisation from AAA server. User configures application through the client. The serving AS can communicate with PIN element, e.g. to collect and process data locally.

### 5.6.4 Post-conditions

The user can install and use a different UE application supported by the service provider. The service provider deploys corresponding AS in PIN. Suitable AS include all kind of applications acting on privacy sensitive data, and, when the client UE is at home or close to home, latency sensitive rendering or interactive application components for games or office applications.

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

The following potential requirements defined in 3GPP TR 22.858 [6] partly cover the use case functionality:

[PR. 5.4.6-001] The 5G system shall be able to support efficient routing, without going through the 5GC, for the communication between a UE and a non-3GPP device, via the residential gateway and an indoor small base station connected to that residential gateway.

[PR. 5.5.6-001] The 5G system shall be able to provide E2E QoS control for the communication path between the UE and a residential gateway via an indoor small base station.

[PR. 5.5.6-002] The 5G system shall be able to support efficient routing for communication between UEs via a residential gateway without going through the 5GC.

[PR. 5.5.6-003] The 5G system shall ensure the use of a residential gateway does not compromise the security of any PLMN or broadband access network.

[PR. 5.5.6-004] The 5G system shall ensure the use of a residential gateway does not compromise the security of the UE.

[PR. 5.5.6-005] The 5G system shall enable the network operator associated with a residential gateway to control the security policy of the residential gateway.

The following 3GPP solutions are incompatible with this use case as they address different areas of the 3GPP system architecture:

3GPP TS 23.548: 5G System Enhancements for Edge Computing: Figure 4.3-1 in clause 4 defines the reference architecture and connectivity models for Edge Computing support in the 3GPP system.

3GPP TS 23.558: Architecture for enabling Edge Applications (EA). This specification defines the application enablers for Edge Computing.

### 5.6.6 Potential New Requirements needed to support the use case

[PR 5.6.6-1] Subject to the PIN being connected to the 5G Network,the 5G system shall be able to provide support for a PIN element discover and access an application on another PIN element. Discovery mechanisms are needed both inside the PIN and to UEs connected to the 5G network, e.g., PIN elements in other PINs, subject to the PIN being connected to the 5G Network.

NOTE: Discovery mechanisms on PIN elements when there is no connectivity to the 5G system may also be needed.

[PR 5.6.6-2] Based on operator policy and subject to the PIN being connected to the 5G network, the 5G network shall be able to support routing of data traffic between a PIN element and an application on another PIN element.

[PR 5.6.6-3] Subject to the PIN being connected to the 5G network, the 5G system shall be able to support QoS for access by a PIN element to an application on another PIN element.

[PR 5.6.6-4] Subject to the PIN being connected to the 5G network, the 5G system shall support a secure mechanism for a PIN element to access an application on another PIN element.

## 5.7 Tour Guide Use case

Editor’s Note: Terminology needs to be aligned with other usecases

### 5.7.1 Description

There are many attractions around the world that are very popular with tourists. Some of the things to see at an attraction have a lot of history or a lot information to be convey about it e.g. how it works etc. In order to help the tourists and provide them with more information tourists can participate in tours, be they either audio tours where by the tourist is given a digital media player, the digital media player being configured for the tourist language or a personalised tour where a tour guide provides a description. In the latter case the tour guide probably gives the tour in one language and can also answer questions.

In both the audio tour and tour guide tour a headset and digital media device are provided to the tourist. The headsets and media devices are usually all the same meaning that the tourist is unfamiliar with how they operate. In addition, a large number of these need to be maintained by the tour company including spares in case there are operational problems. Batteries also need to be charged. When digital media device is provided if additional information for tourists needs to be added / removed all of the digital media players need to be updated.

This use case looks at how a user with a smartphone and set of wearable devices can participate in a tour without specialised equipment.

### 5.7.2 Pre-conditions

Each tourist has a smartphone (UE) (PIN Element) and at least one of smart earbuds and eye glasses (additional PIN Elements). The later 2 are collectively known as wearables. The collection of all 3 is known as a Personal IoT Network. The earbuds and eye glasses communicate wirelessly using PIN direct connections. Tourists use their PINs for listening to music, watching videos and having messenger application video and phone calls. The earbuds will play notifications, sound and the eye glasses will display video images and notifications.

A tour guide has a smartphone (UE), smart earbuds and eye glasses. The earbuds and/or eyeglasses may be IoT devices that communicate with the UE within the PIN.

In popular tourist destinations the Quality Tour Guide (QTG) has a Service Level Agreement (SLA) with service provider C to ensure that the tour guide tours are of the best quality. QTG has been authorised by service provider C to be able to add tourists into QTG PIN. Service provider C also ensures that the security of the service provided to QTG is such that those that have not been authorised by QTG to join the group cannot hear or see QTG tour. Cheaper Tour Guide (CTG) has the same equipment but does not have an SLA, they cannot guarantee a high level of security as QTG can to their tour participants.

### 5.7.3 Service Flows

Terracotta Warriors is a very popular place in China where millions of visitors go each year. Peng (uses service provider A) and Pan (uses service provider B) have decided to visit and are going to take a tour with Quality Tour Guide (QTG) (uses service provider C). They also invite their friend Adrian (uses service provider D from another country, data roaming is turned off) to join. While Adrian is on his way to meet his friends he listens to music on his earbuds from his smartphone.

Meanwhile Pongo and Poppet have also decided to visit but have decided to take a tour with Cheaper Tour Guide (CTG).

When Peng, Pan and Adrian arrive at QTG their earbuds provide a notification sound and the smart glasses provide a visual indication that QTG service is available. They all acknowledge on their smartphone that they authorise QTG to provide the service. In the authorisation information collateral provided by QTG it indicates that QTG has no access to personal information from tour participants (e.g. phone number, IMEI, UICC ID etc) however QTGs service provider will have access to such information for quality assurance purposes. The collateral also indicates that QTG requires access to microphone, earbuds and display capabilities. Pan further configures the service so that he can get notifications from all his other services while Peng has chosen to not be disturbed while in the tour. Adrian has no data service and can only participate in the tour offered by QTG but can still listen to his music. QTG is notified that 3 tourists are ready for a tour and sees a picture of them on their headset.

Pongo and Poppet arrive at CTG where they scan a QR code for the CTG service. CTG receives notification that 2 tourists are ready for a tour.

QTG and CTG take their respective tourists to the 1st sight of a clay warrior. It is very busy at the exhibit with lots of tourists and other tour guides giving their tours. QTG, and CTG give basically the same tour. At this exhibit they provide a verbal description of the clay figure, provide some pictures of the clay figure being excavated and small video clip from the farmer who discovered the clay figure. As Peng, Adrian and Pan listen it is just like standing next to the tour guide with no other tourists, the audio quality is superb. As the pictures are displayed on the smartglasses with some audio description the video then starts to play and can be seen on the smartglasses. Suddenly Pan receives a notification on the glass’s and less pounced notification tone of a WeChat group message, it is from their manager Fei who wants to talk to Pan and Peng. Peng does not get the notification as he has opted not to be disturbed. Adrian has no other service apart from the tour. Pan receives a messenger application call from Fei, the audio from the video display is muted and the messenger application is received from the smartphone UE. Pan walks into a huge metal structure, as Pan is on the messenger application call all of the sudden the call stops. Pan looks at his phone and notices that there is no cellular service.

While Peng, Adrian and Pan were having their tour Poppet and Pongo were receiving the same type of tour from CTG. Poppet and Pongo's audio quality was not as good as Peng and Pan’s, and when the video stream was playing at times the sound would be lost or a video frame corrupted. The problems seemed to get worse when there were more people around, especially when it got very crowded.

Later that week QTG receives a bill from service provider C indicating that 3 tourists used the service for time Y and consumed Z bytes of data.

### 5.7.4 Post-conditions

Service provider C is provided with a set of records indicating that QTG used a specific amount of PIN data.

Service provider C is provided with the identities of the UEs that joined QTG PIN.

All the individuals had successful tours.

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

3GPP TS 22.261 [2] clause 6.9.2 contains requirements for UE communications with the 5GS using a relay and direct device communications.

3GPP TS 22.261 [2] clause 6.3 contains requirement

- The 5G system shall support the capability to operate in licensed and/or unlicensed bands.

3GPP TS 22.101 [3] clause 26a.

### 5.7.6 Potential New Requirements needed to support the use case

[PR 5.7.6-1] The 5G system shall support that a PIN Element may be a member of more than one Personal IoT Network.

[PR 5.7.6-2] The 5G system shall support a PIN Element being added or removed from a PIN by an authorised 3rd party.

[PR 5.7.6-3] The 5G system shall enable PIN direct communications between PIN Elements in a PIN to use licensed spectrum (under the control of a MNO) or between PIN Elements to use unlicensed spectrum (may be under the control of the MNO, or not).

[PR 5.7.6-4] The 5G system shall be able to provision PIN Elements that have been authorised to use that PIN with the necessary configuration parameters to use that PIN subject to MNO and local policies.

[PR 5.7.6-5] The 5G system shall be able to support a PIN Element shall be able to concurrently use both operator managed and non-operator managed PIN direct connectivity with another PIN Element.

[PR 5.7.6-6] The 5G system shall be able to support that a PIN Element can support concurrent communications with PIN Elements in more than one PIN.

[PR 5.7.6-7] The 5G system shall be able to provide secure communications between PIN Elements in a PIN or across different PIN.

## 5.8 Use case support of broadcast-based service discovery

### 5.8.1 Description

In a home network, services are provided for e.g. home automation and wireless hi-fi, which often are based on e.g. UPnP/DNLA, Bonjour and other protocols that can make extensive use of discovery and other broadcast-type messages. The user wants to be able to use the service via both the home network (e.g. Wi-Fi) as well as via the public network.

Several services make extensive use of broadcast messages, e.g. smart home systems. The status or discovery-like messages in e.g. UPnP/DNLA, Bonjour and other protocols are broadcast to all 'participating' IoT devices in the network. This is less of a problem when the service is used in a home network (e.g. via LAN) only. However, when the PIN is used outside the home network via a public network (e.g. smartphone joins the PIN via the 3GPP Network), the phone still receives all broadcast messages. This can cause increased messaging to the UE, while these messages are not always relevant to the user.

The user should have the choice to receive discovery and status messages on demand, or filtered (e.g. only when there is a status change) when using the service via the public network.

Furthermore, the 5G system needs to ensure that the service discovery messages are authentic and sent in sufficiently low numbers as to be not present an obstacle to useful transmissions within the PIN.

### 5.8.2 Pre-conditions

The following pre-conditions apply to this use case:

- IoT devices and the residential gateway are connected to an in-home network

- Service discovery protocols are used to discover services, provide service control and exchange service status

- The residential gateway has a subscription to the 5G system

- IoT devices do not have an individual subscription to the 5G system

### 5.8.3 Service Flows

Mary has a smart home system in her home, in which wireless hi-fi systems (IoT device) are connected to a media server (IoT device) via a non-3GPP wireless radio technology in an in-home network. The IoT devices use a broadcast-based service discovery to find other IoT devices in the network. If Mary wants to control the IoT devices in this smart home system, she uses her smartphone which is also connected to the same in-home network.

Mary is in her living room and wants to turn on the hi-fi system to listen to music from her media server. Mary can easily do this using her smartphone.

It is a nice day outside and Mary decides to sit in the garden. Mary wants to listen to the music outside but cannot hear the music, so she tries to change the volume of the wireless hi-fi system using her smartphone. However, Mary discovers that she is using the public network instead of the in-home network, and therefore cannot control the smart home system using her smartphone.

Mary is unhappy with the situation and therefore she purchases a solution from her network operator that allows her to control the wireless hi-fi system via the public mobile network using her smartphone.

Now she can control the music from her smartphone, even when she is outside. Fortunately, the operator solution filters the broadcast traffic, so that these broadcast messages are not counted for the amount of data she is sending via the mobile network.

### 5.8.4 Post-conditions

The person can control the wireless Hi-Fi system **indoor and outdoor**, usingboth in the in-home network and via the public mobile network (PLMN).

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

3GPP TS 22.261 [2] specifies service discovery for UEs, but not in the context of a PIN.

### 5.8.6 Potential New Requirements needed to support the use case

[PR 5.8.6-1] The 5G system shall enable service discovery of PIN Elements (e.g. based on certain device applications) in PIN by UEs in the PIN or via the public network.

[PR 5.8.6-1a] The 5G system shall enable an authorized PIN user to configure which UEs connected to the public network can perform service discovery of PIN Elements in a PIN. The 5G system shall support configuration per 5GLAN VN, per group of UEs, or per individual UE.

[PR 5.8.6-2] The The PIN Element with gateway capability shall support optimization ofservice discovery of PIN Elements in a PIN by UEs on the public network, e.g. by reducing the amount and frequency of service discovery messages sent from PIN Elements.

[PR 5.8.6-3] The 5G system shall support a mechanism(s) to mitigate a malicious flood of service discovery messages.

[PR 5.8.6-4] The 5G system shall support a mechanism(s) to mitigate spoofing of service discovery messages.

## 5.9 Adding personal health devices to PIN

### 5.9.1 Description

Due to the increasing costs and pressure on the healthcare system, care providers, insurance companies and people themselves are looking at new ways to monitor their health, and manage people’s health remotely. One way this could be achieved until now is that people buy for example a smartwatch or step counter themselves, pair it to their phone, and download an application to their phone to monitor some of their health data. As the requirements for these devices are getting more demanding, requiring to monitor additional physiological data with higher accuracy and improved reliability, and moving towards cloud/edge based analysis of these streams of data, also the requirements on the underlying network connections and manageability of these devices gets more demanding. It also should be made as easy as possible for the user to be able to connect and manage these networked health devices.

In this use case, Fred has been feeling exhausted in the last weeks and went to his general practitioner for a check up, The general practitioner performed a thorough exam and told Fred that he is quite worried about his health, given that his blood pressure is way too high, his cholesterol is at alarming levels, and that he has initial signs of diabetes and heart problems. If Fred continues like this, he has a serious chance of heart failure or ending up in the hospital. Next to some medicines, his general practitioner subscribes him to a new program offered by his insurance company in cooperation with a health provider to monitor Fred’s health. This new program includes a 24/7 wearable monitoring device combined with a cloud service operated by the health provider for early detection and warning of heart arrythmia and heart failure and hypertension. The device will be sent to Fred’s home in a few days.

### 5.9.2 Pre-conditions

Fred has a 5G enabled mobile phone UE with a USIM and a valid 5G subscription, and supports the PIN gateway UE function. Fred also has a Wi-Fi Access Point at home that may be integrated in or associated with a residential gateway connected to the 5G network.

The 24/7 wearable monitoring device uses non-3GPP RAT (e.g. Wi-Fi) and may not be equipped with a (e)UICC.

This use case assumes that the health provider has an SLA with Fred’s mobile operator and that the insurance company either pays or allows Fred to get reimbursed for any additional data or subscription extensions.

### 5.9.3 Service Flows

Fred receives a package that includes a 24/7 wearable monitoring device from his insurance company. The package also includes a set of instructions to follow. All he has to do is use the camera on his 5G enabled UE to scan a QR code on the wearable monitoring device (or e.g. touch the device with NFC).

Fred unpacks the 24/7 wearable monitoring device and scans the QR code using his 5G enabled UE, acting as a PIN gateway UE. Upon doing this, a sequence of events is initiated, which includes the provisioning of credentials (and other configuration information) onto the 24/7 wearable monitoring device enabling it to setup an identifiable connection to an application server through the 5G core network to which the 5G enabled UE is connected.

The connection may be an indirect network connection through the 5G enabled UE, and may be operated by a slice that offers the QoS and reliability guarantees required for this application. In order to facilitate that the 24/7 wearable monitoring device can always connect to the application server, without requiring the 5G enabled UE to be always available or nearby (e.g. wearing the 24/7 wearable monitoring device under the shower, in bed or when the 5G enabled UE is out-of-energy), the 24/7 wearable monitoring device also gets temporary credentials to allow the device to temporarily disconnect from the 5G enabled UE and directly connect to the 5G core network via non-3GPP access to communicate with the application server.

NOTE 1: The direct network connection via non-3GPP access could be enabled e.g. via a trusted network access entity, such as a managed residential gateway or a non-3GPP interworking function. This direct connection does not necessarily need to be permanently enabled, e.g. only be valid when the 24/7 wearable monitor device can temporarily not connect via the 5G enabled UE or when the signal between the 24/7 wearable monitor device and the 5G enabled UE is weak, or only be valid as long as the 5G enabled UE can once in a while update the credentials or validate that the 24/7 wearable monitor is still within operating range.

NOTE 2: The wearable monitoring device can start beeping if it has not been in range of the gateway UE before the credentials expire. The device can also beep if it gets out of coverage of both the gateway UE and AP.

NOTE 3: how the 24/7 wearable monitor device gets paired with a Wi-Fi access point is not in scope of this use case

### 5.9.4 Post-conditions

The data from the 24/7 wearable monitoring device is continuously sent to the application server through the 5G network. Fred feels very safe knowing that his health is constantly being monitored.

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

**From TS 22.261 [2]** "**Service requirements for the 5G system**"**:**

The connection between a remote UE and a relay UE shall be able to use 3GPP RAT or non-3GPP RAT and use licensed or unlicensed band.

The 5G system shall support a secure mechanism for a home operator to remotely provision the 3GPP credentials of a uniquely identifiable and verifiably secure IoT device.

* *Note that the above requirement only partially covers the above mentioned uses case. 3GPP currently relies on the external GSMA remote provisioning framework to perform this function. However, the remote provisioning framework requires a (e)UICC to be supported on the UE, which is not required in this use case. This requirement may need to be further clarified or additional requirements may need to be added to cover non-UICC, non-3GPP RAT devices and the use of a gateway UE to be involved in the provisioning or communication.*

**From TS 22.101 [3]** "**Service aspects; Service principles**"**:**

The 3GPP network shall be able to provide a User Identifier for a non-3GPP device that is connected to the network via a UE that acts as a gateway.

The 3GPP network shall support to perform authentication of a User Identity used by devices that are connected via a UE that acts as a gateway.

A subscriber shall be able to link and unlink one or more user Identities with his 3GPP subscription.

The User Identifier may be provided by some entity within the operator’s network or by a 3rd party.

The 3GPP system shall support to interwork with a 3rd party network entity for authentication of the User Identity.

The 3GPP system shall support to perform authentication of a User Identity regardless of the user's access, the user's UE and its HPLMN as well as the provider of the User Identifier.

The 3GPP system shall support user authentication with User Identifiers from devices that connect via the internet; the 3GPP system shall support secure provisioning of credentials to those devices to enable them to access the network and its services according to the 3GPP subscription that has been linked with the User Identity.

NOTE: it is not clear whether this requirement only covers provisioning of devices that are already properly configured to have a working internet connection or not. For this use case the PIN Element may initially only be able to set up a direct device connection with the gateway UE for onboarding, but it may not have a fully working internet connection. Therefore, this requirement may require further clarification. It may also need to be clarified that the PIN Element may be a headless device.

### 5.9.6 Potential New Requirements needed to support the use case

[PR 5.9.6-1 The 5G system shall support access to the 5G network and its services for an authorized PIN Element (linked to a 3GPP subscription and provisioned with credentials) via a PIN Element with gateway capability or directly via non-3GPP access.

## 5.10 Personal health monitoring PIN Elements

### 5.10.1 Description

Personal health monitoring devices are becoming more readily available to consumers and may be used by doctors to provide remote monitoring of patients. Doctors may provide the devices to their patients and ask the patients to regularly upload measurements to the doctor’s office.

### 5.10.2 Pre-conditions

The personal health monitoring devices are PIN Elements that are designed to provide patient data to the doctor’s servers via the 5G network through a gateway UE. The devices belong to doctors and/or hospitals, who are the owners of the devices, and are configured to use both cellular access networks as well as wifi networks. The devices are configured by the doctor’s office or hospital with credentials belonging to the doctor or hospital to enable communications over the cellular network. Since the devices may be re-used for different patients at different times, the credentials must be offboarded and onboarded properly to ensure the collected data is associated with the correct patient. The devices can also use PIN direct connection to communicate with other PIN Elements in the network.

John has recently suffered from a heart attack and is recovering from treatments in a hospital. Before John is discharged, his cardiologist provides a heart rate monitoring device that he can use so the doctor can monitor his heart rate while doing light exercises at home. While at the hospital, the staff shows John how to associate the device with his smartphone so the device can send data to the doctor’s office server through the smartphone using the cellular network. John needs to also participate in a cardiac rehabilitation program at a local clinic where nurses can monitor his heart rate when he participates in a medically supervised exercise program. He attends the clinic 3 days a week and for other days of the week, John is encouraged to exercise lightly at home. While at the clinic, the heart rate data is shared with the clinic, which is reported back to John’s doctor. He uses the heart rate monitoring device provided by his doctor to record his heart rate while exercising at home and also when he is resting. However, John needs to be careful to maintain his heart rate within a safe range as to not overextend his heart and trigger another heart attack. To ensure the data can still be sent to the doctor’s office in case there is an issue with John’s smartphone, John also associate the device with his spouse’s smartphone. This would provide redundancy for when John is walking outside.

John also suffers from diabetes and his endocrinologist has provided him with a glucose monitoring device. The glucose monitoring device is a PIN Element that is configured with credentials belonging to his endocrinologist so that measurements from the device can be sent to the endocrinologist’s servers via the 5G network. Similar to the heart rate monitoring device, credentials must be offboarded and onboarded to ensure the collected data is associated with the correct patient. John needs to measure his glucose levels before and after each meal and sometimes on-demand if requested by his endocrinologist or when John experiences unusual symptoms. John needs to maintain his blood sugar level above a certain level to avoid experiencing hypoglycemia symptoms such as dizziness, trembling, weakness, seizures, or even loss of consciousness.

Since both the heart monitoring device and the glucose monitoring device may provide measurements that indicate a life-threatening situation, the devices are configured to provide redundant access to the 5G network to ensure John’s doctors are notified in case the measurements are beyond safe levels. The devices are configured to be able to connect to multiple gateway UEs to provide concurrent access for the devices to send measurements to his doctors in case of emergency. The devices can connect to and send measurements through both John’s smartphone and his spouse’s smartphone in addition to connecting to and sending measurements through his home network.

When John visits his daughter’s house, he brings both the heart rate monitoring device and the glucose monitoring device so he can continue to provide measurements to both his doctors. The PIN Elements may communicate concurrently to the gateway UE at his daughter’s house (if one is available) John’s smartphone, and his daughter’s smartphone if an emergency arises. Either way, the data traffic sent from each device is charged to the respective doctor’s. servers (PIN Elements).

NOTE: The sensor measurements (heart rate, sugar levels etc) could be sent over multiple connections at the same time or the sensor is informed that connectivity is unavailable by one route and chooses an alternative route. The mechanism would be dependent on how life threatening the lack of communicating information is.

### 5.10.3 Service Flows

John brings the PIN Elements that were provided by his doctors to his home and connects them to his home network.

- Each PIN Element connects to the home network and to other gateway UEs

- A gateway UE allows the PINs within the home to connect to the 5G system

- Each PIN Element sends data through the gateway UE and the 5G system to the corresponding doctor’s servers

- The 5G system is able to identify what PIN Elements sent each piece of data and generates charging records accordingly

### 5.10.4 Post-conditions

John’s doctors are able to monitor his health remotely through the measurements provided by the PIN Elements.

John doesn’t need to see his doctors as often as he recovers and if his vitals show he is relatively in good health.

The 5G system can correctly identify traffic sent by each PIN Element and generate the appropriate charging records.

The 5G system can provide network access for PIN Elements in medical emergency situations.

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

From 3GPP TS 22.101 [3],

The 3GPP system shall be able to provide User Identities with related User Identifiers for a user.

The User Identifier may be provided by some entity within the operator’s network or by a 3rd party.

The 3GPP network shall be able to provide a User Identifier for a non-3GPP device that is connected to the network via a UE that acts as a gateway.

From 3GPP TS 22.115 [7],

The 3GPP system shall be able to create charging data containing the User Identifier and the subscription to which it is linked for access and use of network services by a non-3GPP device that was authorized with its User Identifier linked to a subscription.

### 5.10.6 Potential New Requirements needed to support the use case

[PR 5.10.6-1] A PIN Element may be a member of more than 1 PIN.

[PR 5.10.6-2] A PIN Element shall be aware in case of loss of its connectivity to 5GS.

[PR 5.10.6-3] The 5G system shall support a PIN Element to be configured with credentials of multiple user identities.

[PR 5.10.6-4] The 5G system shall support access to the 5G network and its services for an authorized PIN Element (linked to a 3GPP subscription and provisioned with credentials) via one or more PIN Element with Gateway Capability.

[PR 5.10.6-5] A PIN Element with Management Capability shall be able to assist a PIN Element that lost its connection to the 5G network in establishing a connection to another PIN Element with Gateway Capability.

[PR 5.10.6-6] A PIN Element shall be able to discover PIN Elements with Gateway Capability and PIN Elements with Management Capability.

## 5.11 Dynamic creation of an on-demand PIN at home

### 5.11.1 Description

Nowadays, most of the operators and smartphones provide a personal hotspot service, which allows the phone to become a WLAN hotspot that provides internet connections to other devices via the UE’s mobile connections. But this only provides internet connectivity to those devices while the smartphone only acts as connection gateway. With the deployment of PIN and the support of the Mobile operators to use this as a new added value service, authorized mobile devices, such as smartphones, tablets, CPEs can be also used as a PIN gateway to dynamically create and manage an on-demand temporary PIN. This on-demand PIN will not only provides connectivity to the devices in the proximity, but also provides more flexibility and authority to the PIN-user to manage the PIN, such as to decide which devices to be connected into this PIN; to manage the service and the traffic within the PIN, so on.

The PIN uses licensed spectrum as well as unlicensed spectrum, Therefore, the creation and management of this type of on-demand PIN requires the authorization and supervision from the PLMN that owns the license spectrum. The PLMN can offer this new on-demand PIN service in certain constrained locations for authorized users with authorized devices. Although the on-demand PIN is provided and controlled by the PLMN, the authorized user of the on-demand PIN can have certain flexibility to manage this PIN, such as to decide when to create and terminate the PIN, coordinate with PLMN to authorize the devices to be allowed to access this PIN, manage the services being allowed in this PIN, so on.

### 5.11.2 Pre-conditions

Tom is an avid game player and his local operator M offers a service where by the operator allows a customer to create on-demand PIN and download games to PIN element(s) with gateway and management functionality (e.g. 5G home access router as example in this use case, but it can also be a mobile phone so that the players can create a gaming session everywhere, e.g. at the school yard or in the park), the home access router is provided by operator M and supports device connectivity using a variety of access technologies (e.g. operator managed 3GPP RAT, WLAN, Bluetooth®). Collectively operator M calls this “PIN Functionality”

NOTE: These variety of access technologies are supported as avid game players usually have a variety of new and old devices they want to use.

The 5G home access router also stores games meta data that can be uploaded Operator’s M network so that the game can be played later on other PIN element(s) or the same 5G home access router at different location.

Today is the game night, Tom invites his friend Mike, James and Howard to his house to try the new air-combat video game that he just bought recently. The air-combat video game provider has partnership with the Operator M which hosts the game edge server in its network. Tom installed a local version of the game applicationin the 5G home access router.

Mike, James and Howard bring their own wireless game consoles as well as wireless VR glasses. Mike, James’s console and VR glasses are 5G capable of supporting 26GHz spectrum with the subscription of operator M. Howard has the subscription of Operator A for his 5G game console which also support WLAN and Bluetooth®. Howard also has a VR glass which can link to his 5G game console with PIN direct connection, such as Bluetooth®.

### 5.11.3 Service Flows

1 After his friends arrive, Tom turns on its PIN function in his 5G access router. This 5G router sends on-demand PIN creation authentication and authorization request to Operator M, for creating a PIN in this device for 4 hours in his house using mmWave spectrum owned by M. Per the subscription Tom bought, the maximum number of devices to be allowed in this PIN is 10, and tonight he only requires 8 devices. Because the on-demand PIN subscription which Tom bought is the basic and only allows local traffic, it means that guest devices in this PIN will not be able to access services outside the PIN. The PIN subscription also has other restrictions, such as the PIN only allowed operating in Tom’s house and for maximum 10 hours for each time the PIN being created.

NOTE: Basic+ is the same as Basic subscription but allows devices, if supported, to use operators managed spectrum. Tom upgraded tonight because in the past when Mike and others came over and they just used non 3GPP access technologies sometimes there was too much delay and parts of games became unplayable.

2 After being authorized by M, this 5G home access router is reconfigured by PLMN remotely, which may include getting some necessary functions downloaded from M, to be able to act as PIN gateway.

3 When the 5G home access router is ready, it starts to use and broadcast its own PIN network ID which can be assigned by M or named by Tom depended on the M’s policy.

4 Mike and James have connected to Tom’s game night PIN before on other game nights, so their devices automatically discover and connect their 5G home access router and VR glasses to this PIN after being authenticated & authorized via Tom’s 5G home access router. It’s Howard first time to use PIN since he has no subscription of M, he has to manually select and connect his game console to “game night “ PIN using WLAN.

5 An local game server is created and hosted in the 5G router after the PIN is up, so everyone’s game consoles can be connected to that local game server for playing locally. Before coming to Tom’s house, James played the game at his home and his game console was connected to the game server hosted in the PLMN’s cloud. After being connected to “game night” PIN, James’s connection with the game server is relocated to the local game service in the “game night” PIN. Within this PIN, Tom, Mike, James’s game consoles and VR glasses can communicate with each other using direct device communication with the26Ghz spectrum, while their consoles communicate with the local game server via Tom’s 5G home access router. Howard’s console can communicate with others’ consoles and the local game server via the connection to Tom’s 5G Home access router using WLAN.

6 Tom’s 5G home access router monitors and controls the communication of those devices in “game night” PIN based on the policy from M, also may coordinate with M for some necessary network managements, such as interference management.

7 All the gaming content being exchanged between these players is conveyed locally, only the game status information can be conveyed back to the central game server in the cloud via the local game function in Tom’s 5G home access router.

8 Because the PIN is created for only 4 hours, the service and connections associated with PIN elements as well as operators 5GC are configured accordingly to the lifetime of the PIN, to avoid sudden service disruption when the PIN has ended after time life expires.

9. Tom and Mike are one team to against the team of James and Howard in the game. Tom and Mike establish an encrypted communication between their game consoles to exchanges some private information (e.g. screen shots, game maps, private chat, voice etc), while another secured communication between James and Howard’s devices is also created.

### 5.11.4 Post-conditions

Tom, Mike, James and Howard happily play the game in Tom’s house for 3 hours. After 3 hours, they are so into the game and don’t want to finish in 1 hour and decide to extend the game night for 3 more hours. So, Tom sends the PIN modification request to M to extend the PIN for 3 more hour and is approved. When 7 hour PIN life time expires, all the game consoles and VR glasses have been disconnected from the PIN as well as the game service, then the “game night” PIN is terminated. 5G access route sends the charging information for this 7-hour operation of PIN.

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

### 5.11.6 Potential New Requirements needed to support the use case

Editor Notes: New requirements are for FFS.

[PR.5.11.6-1] 5G system shall be able to support creation / termination / modification of an PIN in certain location for a requested period of time (e.g., hours) with the authorization from the operator based on the subscription of the PIN user.

[PR-5.11.6-2] 5G system shall be able to allow authorized PIN Elements automatically or manually to discover other PIN element(s) for communication.

[PR-5.11.6-3] 5G system shall be able to support authentication and authorization of PIN elements whose subscriptions can belong to different operators to access the PIN.

[PR-5.11.6-4] 5G system shall be able to support secured communications between two or more individual PIN elements within a PIN.

[PR-5.11.6-5] 5G system shall be able to support mechanism to provide life span information of the PIN to the authorized 3rd party or the PIN elements when the PIN is created for limited time span.

[PR-5.11.6-6] 5G system shall be able to support an authorized 3rd party to set policies on which PIN Elements can access which services or PIN elements in an PIN.

PR-5.11.6-7] 5G system shall be able to support an authorized 3rd party to set policies duration of access, IP connectivity type (local break out 5GC etc) local services etc.

## 5.12 Operator managed PIN

### 5.12.1 Description

This use case describes the required support from operator to manage PIN Elements including IoT devices or non-3GPP devices in a PIN, in a home or in an office.

### 5.12.2 Pre-conditions

Bob has a mobile subscription with MNOa.

Bob has a smart home network using a gateway (i.e. a PIN Element with Gateway Capability) that is provided and managed by MNOa.

Bob’s smart home network supports several wireless technologies, including 3GPP direct device connection, WLAN, Bluetooth®, wireline, etc.

The 5G network of MNOa has a list (also referred to as a collection or group) of PIN Elements in Bob’s smart home network, which can be managed by the 5G network. This list is called the list of *managed* PIN Elements. This list contains information for each PIN Element, such as an identity, connectivity capabilities, credentials, communication restrictions (e.g. other PIN Elements it cannot communicate with), etc.

### 5.12.3 Service Flows

Step1: Bob buys a new PIN Element, e.g. a smart plug with WLAN capability.

Step2: Bob connects this PIN Element to the WLAN of his smart home network and the PIN Element obtains an IP address.

Step3: The 5G network of MNOa detects that a new PIN Element is connected to Bob’s PIN.

Step4: The 5G network acting as an Identity provider creates a User Identity and User Profile for the PIN Element based on UIA Framework in TS 22.101.

Step5: The 5G network of MNOa sends a notification to Bob’s UE (a member of the PIN) requesting permission to add this device to the list of managed PIN Elements of his PIN.

Step6: Bob grants permission and the 5G network of MNOa adds the PIN Element to the list of "managed" PIN Elements.

### 5.12.4 Post-conditions

Bob is now able to monitor and control the PIN element (and any other PIN element in the list of "managed" PIN Elements), e.g. by using a web application provided by MNOa.

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

The service requirements in TS 22.101 clause 26a provide the principle for user centric identifiers and authentication by the 3GPP system:

- The 3GPP System shall support operators to act as User Identity provider and to authenticate users for accessing operator and non-operator deployed (i.e. external non-3GPP) services.

This use case and requirements consider that the application running on the PIN Element is a non-operator deployed (i.e. external non-3GPP) services behind a PIN Element with Gateway Capability in PIN.

### 5.12.6 Potential New Requirements needed to support the use case

[PR 5.x.6-1] The 5G system shall support a mechanism for a network operator or authorized 3rd party to create a PIN and manage the PIN Elements for the PIN.

## 5.13 A smart hospital bed as a PIN element

### 5.13.1 Description

Hummel is a 70-year-old cardiac patient who is equipped with a pacemaker at the TeleCare hospital, who have their own 5G network. During the recent remote intervention, the doctors decided that he must admit himself for a surgery to replace the batteries of his pacemaker. In order to monitor the health of his heart continuously, Hummel has received a 5G enabled wearable heart monitor from another hospital, which is capable of continuously monitoring the vitals including the heartrate and send its data via a 5G network to a cloud server. He also has other personal connected health devices such as an SpO2 monitor and a connected insulin pump attached to his body that are wirelessly connected to his mobile phone for complete overview of his health. He also has a special sleep mask enabling him to breathe better during his sleep and monitor the quality of his sleep that is also connected to his mobile phone when he is using it. It is assumed that all his health devices are clinically qualified to be used for diagnosis in a hospital.

Upon arriving at the hospital reception, Hummel is immediately directed to the cardiology department, where a 5G enabled smart hospital bed is allocated for him. The smart hospital bed is configured as a PIN element with gateway capability and with management capability. The smart hospital bed enables personal devices of the patient to be connected to the 5G network of the hospital. It also allows some of the PIN elements connected to the hospital bed, such as some controls over the elevation of the head of the bed and a personal screen connected to the bed (e.g. to watch TV or to stream some video content to watch). The hospital bed is also connected to a high-end patient monitor, located behind the patient. Although it cannot be controlled by the patient, the output of the monitor can be displayed and browsed by the patient on his mobile phone or the attached personal screen.

Upon reaching the smart hospital bed, the devices that are carried and worn by Hummel and the hospital bed (with its connected PIN elements) can discover each other, and together form a PIN. Via the smart hospital bed, the necessary credentials to securely communicate with each other, and to connect to the hospital 5G network are downloaded and configured in Hummel’s devices. The data from Hummel’s health devices can now be sent to the TeleCare’s 5G network, where it can be processed and used for health monitoring by the hospital staff. The high-end patient monitor linked to the smart hospital bed can receive the data from Hummel’s devices directly from the devices and generate an alarm if Hummel’s condition deteriorates. Using the PIN, Hummel can also control the elevation of his bed via his mobile phone and stream some videos from his mobile phone on the screen connected to the bed, and browse the output of the patient monitor.

### 5.13.2 Pre-conditions

Hummel has a 5G PIN enabled mobile phone (i.e. a UE), with several personal health devices wirelessly connected to it. The mobile phone may be a PIN element with gateway capability and/or management capability.

Hummel also has a 5G PIN enabled wearable heart monitor capable of sending its data via a 5G network to a cloud server.

The hospital bed is 5G PIN enabled UE and is a PIN element with gateway capability and/or management capability. For its management capability it may use the attached screen to display a user interface to the user.

TeleCare may function as an NPN, preventing full access to the network services for unregistered devices. TeleCare may deploy not only a single NPN, but may deploy multiple NPNs, e.g. one for staff (with full access to the network services) and one for patients (with limited access to the network services).

### 5.13.3 Service Flows

- Upon entering the cardiology department inpatient room, Hummel’s mobile phone and the smart hospital bed can discover each other. Also the 5G PIN enabled wearable heart monitor and the smart hospital bed can discover each other.

- When Hummel looks at his mobile phone, he notices that it has discovered the smart hospital bed. It also shows the list of connected PIN elements connected to the hospital bed.

- Hummel can connect his mobile phone to the smart hospital bed and upon connecting, Hummel’s mobile phone gets added to the hospital’s bed PIN. Also the personal devices that are connected to Hummel’s mobile phone are discovered by the hospital bed and automatically added to the hospital bed’s PIN.

- On the screen of the mobile phone (or the screen attached to the hospital bed), it also shows that the 5G PIN enabled wearable heart monitor in the list of discovered PIN elements. Hummel presses a button to also add that device to the hospital bed’s PIN.

- After exchange of credentials, the PIN elements can now securely communicate between each other. This allows Hummel to use the screen attached to the bed for streaming some videos from his mobile phone, allows the data from his heart monitor to be received by the high-end patient monitor, and show the patient monitor’s data on his mobile phone.

- As part of the PIN configuration, the PIN elements are also allowed to gain patient access to the hospital network (via the hospital bed’s PIN gateway capability). On the screen of his mobile phone (or the screen attached to the hospital bed), Hummel allows his wearable heart monitor and his other connected health devices to send their data to the hospital network.

- The data from the connected devices are useful in improving the pre-surgical preparation of Hummel and saves operational overhead for the hospital staffs.

- Thanks to the PIN feature, Hummel had an easy transfer to the hospital and had a fairly comfortable experience (despite his condition) in his smart hospital bed.

### 5.13.4 Post-conditions

Upon discharge, the network profiles from his mobile phone, his heart monitor and his personal connected health devices are decommissioned from the PIN and from the hospital network and return to their original operating state.

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

### 

### 5.13.6 Potential New Requirements needed to support the use case

[PR 5.13.6-1] The 5G system shall enable PIN elements to discover and identify each other.

NOTE: this may be done directly (depending on the discovery capabilities of the PIN elements) or via a PIN element with gateway capability or via a PIN with management capability.

[PR 5.13.6-2] The 5G system shall enable PIN elements with management capability to add PIN elements to the PIN.

[PR 5.13.6-3] The 5G system shall allow only authorized PIN elements to connect to the 5G network via a PIN element with gateway capability.

NOTE: next to authorization of the 5G network operator, additional authorization/consent from the PIN user may be needed depending on whether the user wants to allow PIN elements to connect to the 5G network or not.

# 6 Considerations

A lot of the usecases in this document are based on existing systems (e.g. ZigBee® Specification [9], Z-Wave ® [10]]) that can be deployed today, infact the overview identifies two main Personal IoT Networks, wearables and home automation. These existing Personal IoT Networks use a number of different technologies that provide a set of capabilities.

# 7 Potential Consolidated Requirements

This section provides Consolidated Potential Requirements for consideration to include in the normative specifications. The CPR’s have been grouped into different functional categories, each category contains a table that lists the original PR and any relationship to TR 22.858 [6].

## 7.1 Gateway

Table 7.1-1 – PIN Gateway Consolidated Requirements

| CPR No. | Potential Requirement | |
| --- | --- | --- |
|  | Original Potential requirement  No. | Potential requirement text |
| TBD | TBD | TBD |

## 7.2 Service Discovery

Table 7.2-1– PIN Service Discovery Consolidated Requirements

| CPR No. | Potential Requirement | |
| --- | --- | --- |
|  | Original Potential requirement  No. | Potential requirement text |
| TBD | TBD | TBD |

## 7.3 Service Hosting

Table 7.3-1 – PIN Service Hosting Consolidated Requirements

| CPR No. | Potential Requirement | |
| --- | --- | --- |
|  | Original Potential requirement  No. | Potential requirement text |
| TBD | TBD | TBD |

## 7.4 Privacy

Table 7.4-1 – PIN Privacy Consolidated Requirements

| CPR No. | Potential Requirement | |
| --- | --- | --- |
|  | Original Potential requirement  No. | Potential requirement text |
| TBD | TBD | TBD |

## 7.5 Direct Communications

Table 7.5-1 – PIN Direct Communications Consolidated Requirements

| CPR No. | Potential Requirement | |
| --- | --- | --- |
|  | Original Potential requirement  No. | Potential requirement text |
| TBD | TBD | TBD |

## 7.6 Connectivity - QoS - charging

Table 7.6-1 – PIN Connectivity, QoS and Charging Consolidated Requirements

| CPR No. | Potential Requirement | |
| --- | --- | --- |
|  | Original Potential requirement  No. | Potential requirement text |
| TBD | TBD | TBD |

## 7.7 Provisioning

Table 7.7-1 – PIN Provisioning Consolidated Requirements

| CPR No. | Potential Requirement | |
| --- | --- | --- |
|  | Original Potential requirement  No. | Potential requirement text |
| TBD | TBD | TBD |

## 7.8 Positioning

Table 7.8-1 – PIN Positioning Consolidated Requirements

| CPR No. | Potential Requirement | |
| --- | --- | --- |
|  | Original Potential requirement  No. | Potential requirement text |
| TBD | TBD | TBD |

## 7.9 KPIs

Editor’s note: KPI still need to be completed at SA1#95e, this section will be updated then.

# 8 Conclusions and Recommendations

[Editor’s note: Text to be provided at the end of study.]

# Appendix A Connectivity models

## A.1 General

This annex provides a diagrammatic view of the types of connectivity models that are supported in a PIN. Each diagram will contain 2 types of lines, one that shows a PIN Element to PIN Element transport and a second line that shows the end to end communication. In both diagrams PIN Elements use PIN direct connections, however PIN Element to PIN Element end to end communication may require a relay.

A PIN Element may support more than one form of connectivity but this is not shown in the diagrams.

## A.2 PIN direct connectivity with no relay

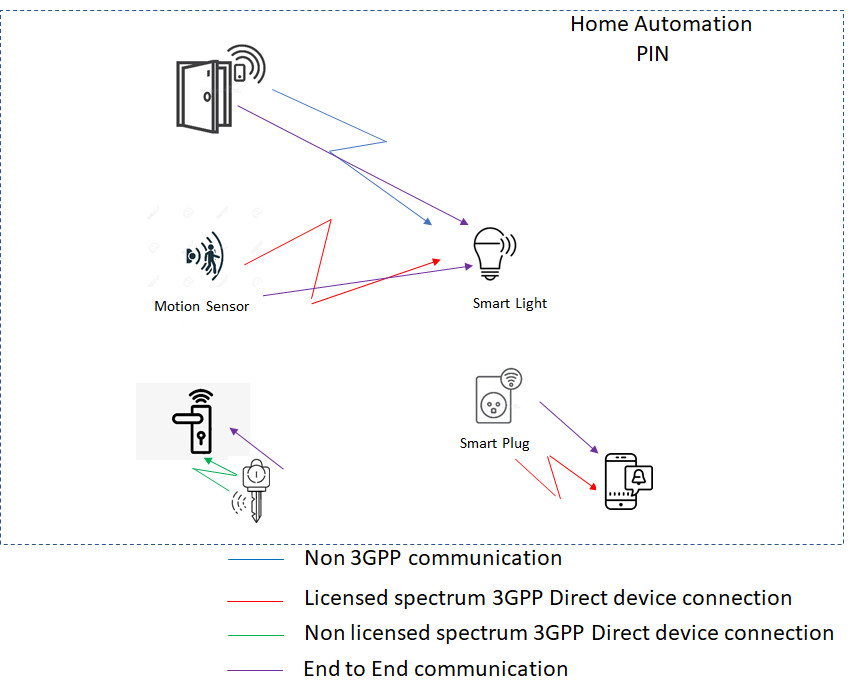


Figure A2-1: Examples PIN direct connectivity in a PIN

Figure A2-1 shows PIN Elements that communicate directly, without any relay elements to another PIN Element, this is collectively known as PIN direct connection. PIN direct connection can encompass different types of direct connection as show in Figure A2-1:

a) Door sensor (a device PIN Element) uses PIN direct connection (e.g. WLAN) to communicate with a light bulb (e.g. door opens and the light turns on).

b) Motion sensor (UE PIN Element) uses PIN direct connection in licensed spectrum to communicate with the light bulb (e.g. motion is detected in the room and the light bulb turns on).

NOTE PIN direct connection in 3GPP licensed spectrum is direct device connection as defined in TS 22.261 [2].

c) The key uses PIN direct connection in non licensed spectrum to communicate with the door lock (e.g. key opens the door).

d) The smart plug (UE PIN Element) uses PIN direct connection in licensed spectrum to communicate with the smartphone (e.g. notification that it is using 60 watts of energy).

## A.3 PIN direct connection using a relay.

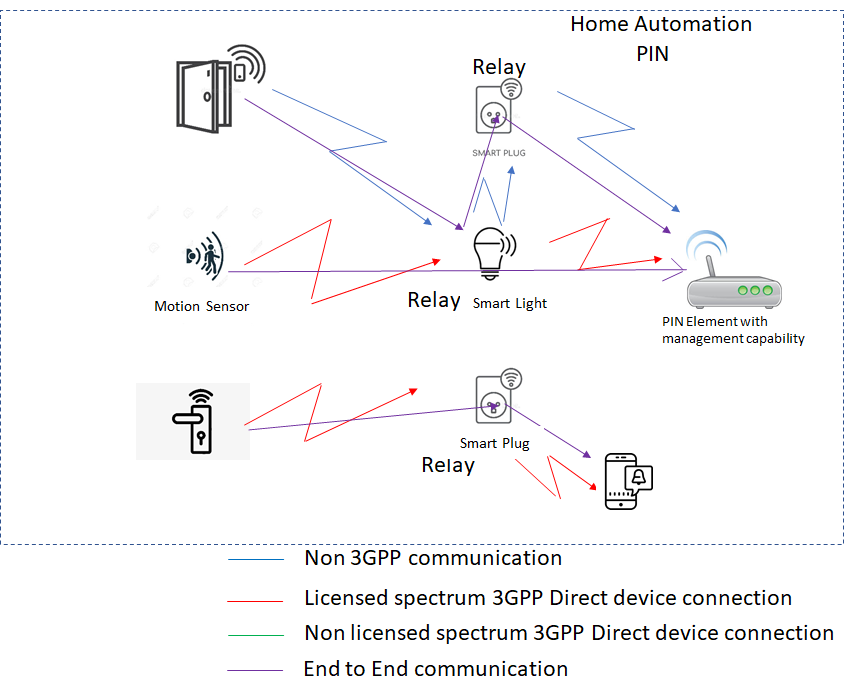


Figure A3-1: Examples PIN direct connection using a relay in a PIN

Figure A3-1 shows PIN Elements that communicate directly but there is a relay in the communication path. Figure A3-1 shows the following:

a) Door sensor (device PIN Element) uses PIN direct connection (Non 3GPP communication) to communicate with a PIN Element with management capability via 2 relays (light bulb and smart switch).

b) Motion sensor (UE PIN Element) uses PIN direct connection in licensed spectrum to communicate with the a PIN Element with management capability via a relays (light bulb) (e.g. to configure the motion sensor to turn the light bulb on or off).

c) The door lock (UE PIN Element) uses PIN direct connection in licensed spectrum to communicate with the smartphone (e.g. notification that it opened) via a relay (smart socket).

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2020-08 | SA1#91e | S1-203283 |  |  |  | TR Skeleton | 0.0.0 |
| 2020-09 | SA1#91e | S1-203390 |  |  |  | Incorporated the following PCRs into TR:  S1-203422, S1-203418, S1-203419, S1-203420, S1-203371, S1-203421 | 0.1.0 |
| 2020-11 | SA1#92e | S1-204360 |  |  |  | Incorporated the following PCRs into TR:  S1-204443, S1-204334, S1-204331, S1-204333, S1-204438, S1-204439, S1-204063, S1-204440, S1-204445, S1-204441, S1-204444, S1-204442, S1-204332, S1-204066 | 0.2.0 |
| 2021-03 | SA1#93e | S1-210314 |  |  |  | Incorporated the following PCRs into TR:**S1-210486, S1-210487, S1-210488, S1-210489, S1-210490, S1-210491, S1-210492, S1-210493, S1-210494, S1-210495, S1-210496, S1-210497** | 0.3.0 |
| 2021-03 | SA#91e | SP-210208 |  |  |  | Presented for information, MCC clean-up | 1.0.0 |
| 2021-05 | SA#94e |  |  |  |  | **S1-211457, S1-211458, S1-211459, S1-211460, S1-211461, S1-211469, S1-211092, S1-211463, S1-211464, S1-211157, S1-211158, S1-211465, S1-211467, S1-211468, S1-211466** |  |

1. An example product <https://manuals.fibaro.com/door-window-sensor-2/> [↑](#footnote-ref-1)
2. Window, door sensors should be secure as they provide information related to the integratory of a building and the security mechanisms used on those communications links should be more secure than those probably on a light bulb, In the case of the sensor credentials are stored by e.g. the sensor vendor whereas the light bulb ones could be on packaging or provisioned in a more an open fashion. [↑](#footnote-ref-2)
3. This is based on calculation done at this website (below). However accurate references need to be provided. Figure has been increased to account for lights, appliances, door bells etc

   https://www.quora.com/How-many-electrical-outlets-exist-in-the-United-States-Or-how-should-I-calculate-this [↑](#footnote-ref-3)
4. Looking for this as a starting point for coding in ASN.1   
   ThreeDLocation ::= SEQUENCE {

   latitude Latitude,

   longitude Longitude,

   elevation Elevation

   } [↑](#footnote-ref-4)