

The vivo logo is positioned in the top left corner of the slide. The background of the entire slide is a dark blue, abstract image with glowing, fiber-like patterns radiating from a central point, resembling a network or a microscopic view of a material.

vivo

# Study on Personal IoT network - UPDATED (PIN)

2021.11

## Summary of moderator email discussion

- PC5 related
  - Almost half number of companies believe PC5 is an important technology to be supported in future by devices, which also is supported by SA1 requirement, and question that study on non-3GPP access is out of SA2 scope. So they think PC5 should not be removed in R18 study.
  - Other companies question the capability of devices supporting PC5 in close future, and for the sake of reducing TUs, propose to study PC5 case in future release.
  - Two companies propose a compromise that R18 only study the access independent method, i.e., study the interaction between PEGC and PIN Elements that is upper layer of the access, which is transparent to the access.
- Way forward
  - In R18 the interaction between PEGC and PIN Elements, if needed, is independent on the access types (non-3GPP or PC5).

## Summary of moderator email discussion (continue)

- Communication path switch related
  - We already have service continuity WT#4, which studies the case that none of the communication peer is changed, while communication path switch is similar as call transfer (an example of call transfer is IMS IuT), which studies the case that one of the communication peer is changed.
  - Most companies believe it is not the right time to study it in R18, this is a feature over the PIN basic services, and we could first have a stable PIN version, then could study whether there's some SA2 impact. This would help to reduce TUs too.
  - Three companies have concern related to PC5/ProSe SID and question the place where to study the solution – R18 PIN or R18 ProSe. As the way forward proposed in 1.1.4, we will study the interaction transparent to access technology, and future we may consider the optimization that has impact on access and where to study the solution. That would remove the concern.
  - There's another possibility to study this in R18, that we can study it in SA6 on application level. In future, we can study whether there will be optimization in SA2 for the transfer.
- Way forward
  - Remove the WT in SA2 R18 SID, and could study it in SA6 R18 SID.

# Updated Objectives

- (WT#1) Architecture enhancement:
  - (WT#1.1) To study the potential architectural enhancements for supporting management of PIN, access of PIN via PIN Element with Gateway Capability (PEGC), and communication of PIN (e.g. PIN Element communicates with other PIN Elements directly or via 5GS or via PEGC and 5GS).
  - (WT#1.2) To study the potential architecture enhancements for supporting identifying PIN Elements in the PIN.
- (WT#2) Security related:
  - (WT#2.1) To study whether identification is needed, and if yes how to identify at 5GC level to serve as a basis for authenticating/authorizing, and charging of PIN elements.
  - (WT#2.2) To study the provisioning and configuration of PIN Element, if supported and needed, by, e.g., a PIN Element with Management Capability (PEMC), for supporting the credential and identity management requirements as defined in TS 22.101 clause 26a.
  - (WT#2.3) To study the mitigation of repeated and unauthorized attempt to access a PIN or PIN Elements in a PIN.
- (WT#3) Management as well as policy and access right enforcement:
  - (WT#3.1) To study the management of a PIN, e.g., create PIN, authorizing/de-authorizing PIN Elements, authorizing/de-authorizing PIN Elements with Management Capability (PEMC), authorizing/de-authorizing PIN Elements with Gateway Capability (PEGC), establishing duration of the PIN, etc.
  - (WT#3.2) To study the procedures for network discovery, PIN Element discovery, capability of PIN Element discovery, as well as availability and reachability discovery, e.g., assisted by a PIN Element with Management Capability (PEMC). Furthermore, to study whether and how to enable the discovery of service provided by PIN Element.
  - (WT#3.3) To study the access right enforcement of communication to support the PIN, e.g. between PIN Elements directly or via 5G core network, and between PIN Elements and 5G core network.
- (WT#4) Service continuity and charging consideration:
  - (WT#4.1) To study the service continuity when a PIN Element, if supports 5GS direct access, moves from direct 5GS access to indirect 5GS access via PEGC or vice versa and charging consideration.

## Updated Timeline

- Expect to start with other Rel-18 studies
  - **4 TUs for study phase and 2 TUs for WI phase**
- Send to SA plenary for information in **SA#96 June 2022**
- Send to SA for approval in **SA#97 Sept. 2022**

# Updated Work Tasks

Work Task	TUs (study)	TUs (normative)
<p>(WT#1) Architecture enhancement:            (WT#1.1) To study the potential architectural enhancements for supporting management of PIN, access of PIN via PIN Element with Gateway Capability (PEGC), and communication of PIN (e.g. PIN Element communicates with other PIN Elements directly or via 5GS or via PEGC and 5GS).            (WT#1.2) To study the potential architecture enhancements for supporting identifying PIN Elements in the PIN.</p>	1	0.5
<p>(WT#2) Security related:            (WT#2.1) To study whether identification is needed, and if yes how to identify at 5GC level to serve as a basis for authenticating/authorizing, and charging of PIN elements.            (WT#2.2) To study the provisioning and configuration of PIN Element, if supported and needed , by, e.g., a PIN Element with Management Capability (PEMC), for supporting the credential and identity management requirements as defined in TS 22.101 clause 26a.            (WT#2.3) To study the mitigation of repeated and unauthorized attempt to access a PIN or PIN Elements in a PIN.</p>	0.5	0.25
<p>(WT#3) Management as well as policy and access right enforcement:            (WT#3.1) To study the management of a PIN, e.g., create PIN, authorizing/de-authorizing PIN Elements, authorizing/de-authorizing PIN Elements with Management Capability (PEMC), authorizing/de-authorizing PIN Elements with Gateway Capability (PEGC), establishing duration of the PIN, etc.            (WT#3.2) To study the procedures for network discovery, PIN Element discovery, capability of PIN Element discovery, as well as availability and reachability discovery, e.g., assisted by a PIN Element with Management Capability (PEMC). Furthermore, to study whether and how to enable the discovery of service provided by PIN Element.            (WT#3.3) To study the access right enforcement of communication to support the PIN, e.g. between PIN Elements directly or via 5G core network, and between PIN Elements and 5G core network.</p>	2	1
<p>(WT#4) Service continuity and charging consideration:            (WT#4.1) To study the service continuity when a PIN Element, if supports 5GS direct access, moves from direct 5GS access to indirect 5GS access via PEGC or vice versa and charging consideration.</p>	0.5	0.25

THANK YOU.

谢谢。

# CONTENTS

**01.**

**Aspects  
within PIRates**

**02.**

**Requirements,  
Scenarios,  
Motivations**

**03.**

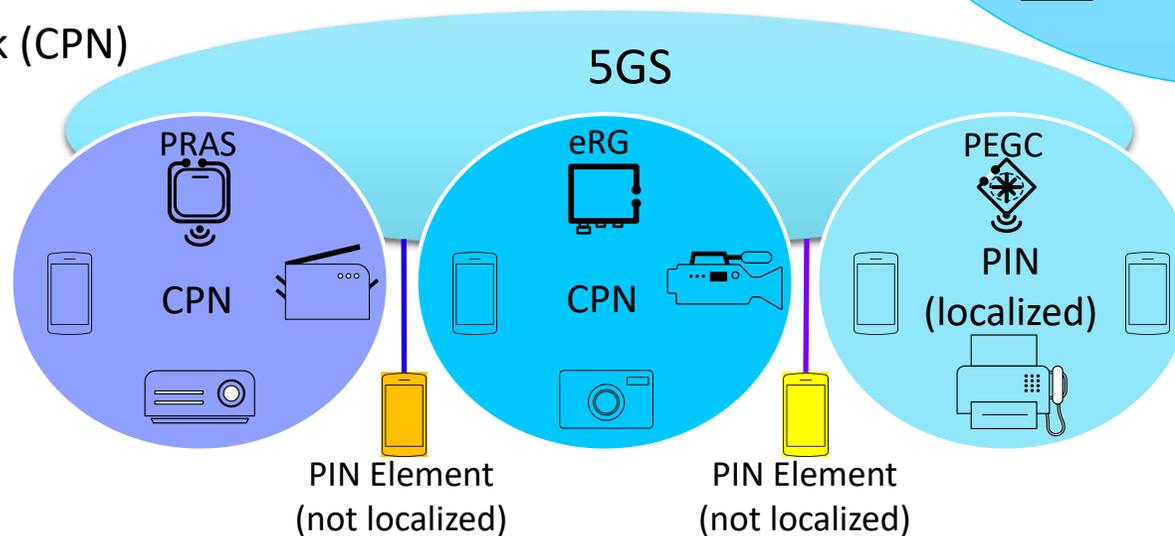
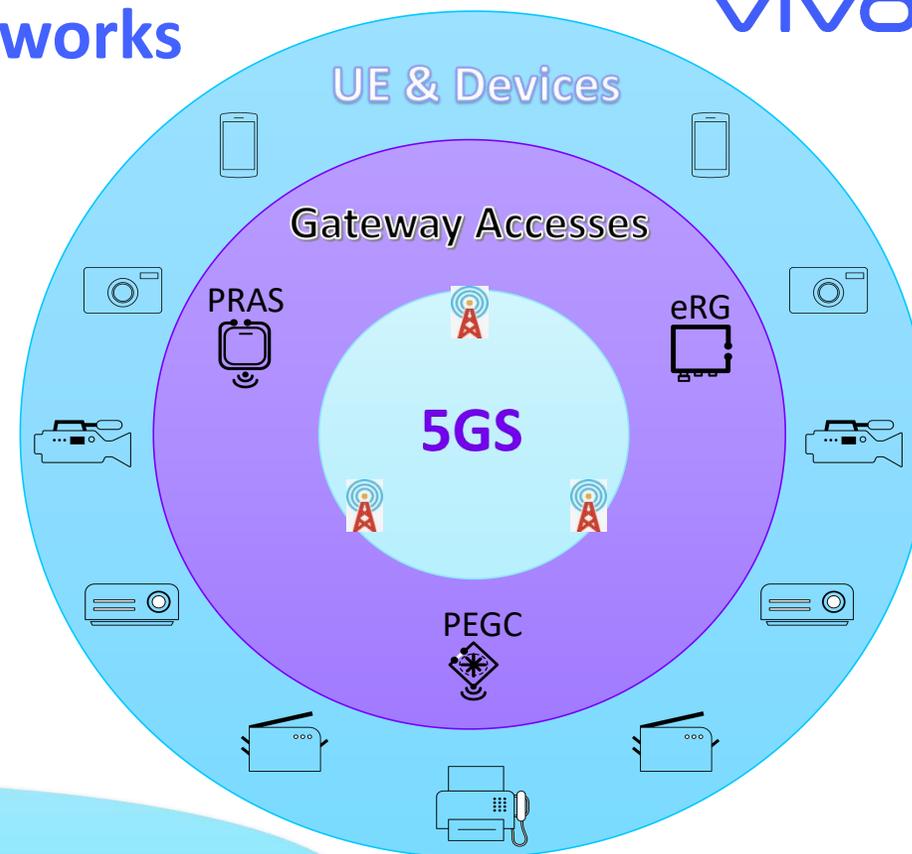
**Objects**

**04.**

**Timeline and  
work tasks**

# Aspects within personal IoT and Resident networks

- Types of gateway
  - PIN Element with Gateway Capabilities (PEGC) (e.g., relay UE)
  - Premises Radio Access Station (PRAS)
  - evolved Residential Gateway (eRG)
- Personal IoT Network (PIN)
  - Localized with PEGC (**at least one within a PIN**)
  - Direct 5GS access (not localized)
- Customer Premises Network (CPN)
  - Localized with eRG
  - Localized with PRAS
  - Localized with PRAS+eRG



**PIRATES**

# CONTENTS

**01.**

**Aspects  
within PIRates**

**02.**

**Requirements,  
Scenarios,  
Motivations**

**03.**

**Objectives**

**04.**

**Timeline and  
work tasks**

# Requirements from SA1

## Access right enforcement for communications and discovery

### Requirements from TS 22.261

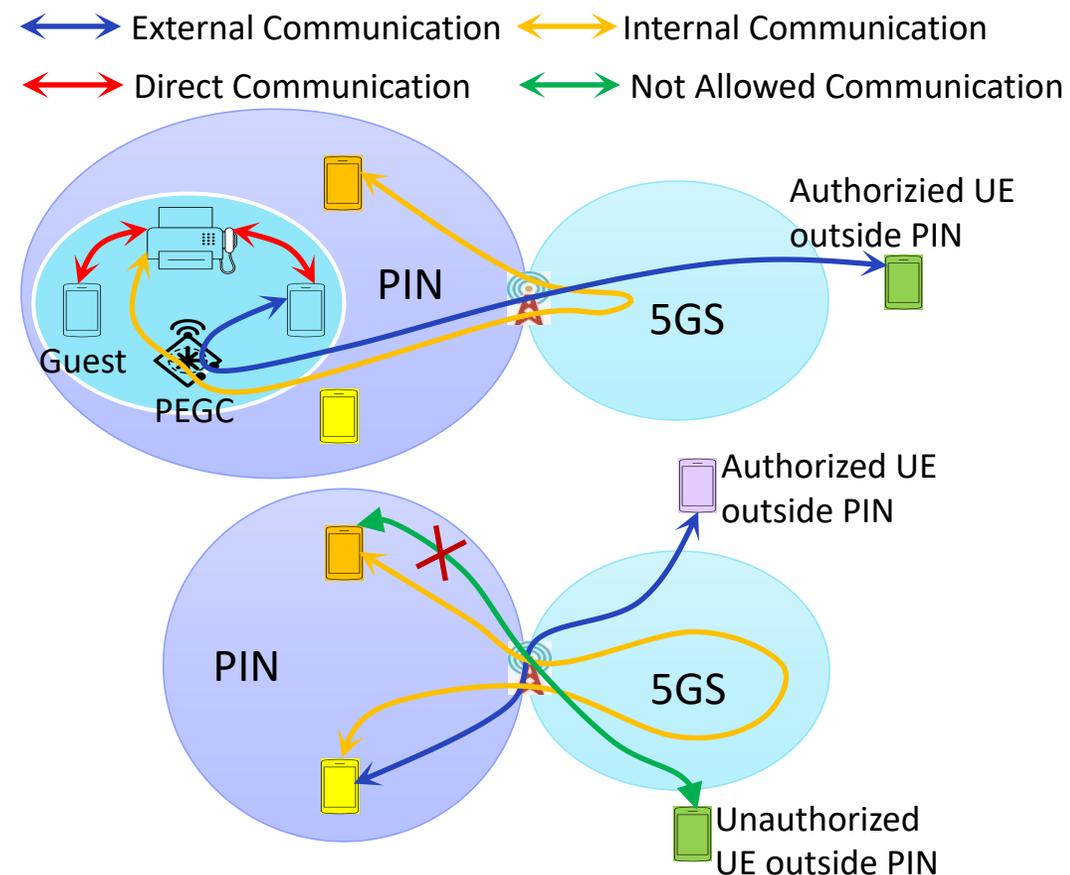
The 5G system shall support mechanisms for a PIN User, network operator or authorized 3rd party to create and manage a PIN, including:

- Authorizing/deauthorizing PIN Elements;
- Authorizing/deauthorizing PIN Elements with Management Capability;
- Authorizing/deauthorizing PIN Elements with Gateway Capability;
- Establishing duration of the PIN;
- Configure PIN Elements to enable service discovery of other PIN Elements;
- Authorize/deauthorise if a PIN Element can use a PIN Element with Gateway Capability to communicate with the 5GS;
- Authorize/deauthorise for a PIN Element(s):
  - which other PIN Element it can communicate with,
  - which applications/service or service in that PIN it can access
  - which PIN Element it can use as a relay.
- Authorize/deauthorise a UE to perform service discovery of PIN Elements over the 5G network;
- Configure a PIN Element for external connectivity e.g. via 5G system;

The 5G system shall efficiently support service discovery mechanisms where a UE or non-3GPP device in a CPN or PIN can discover, subject to access rights.

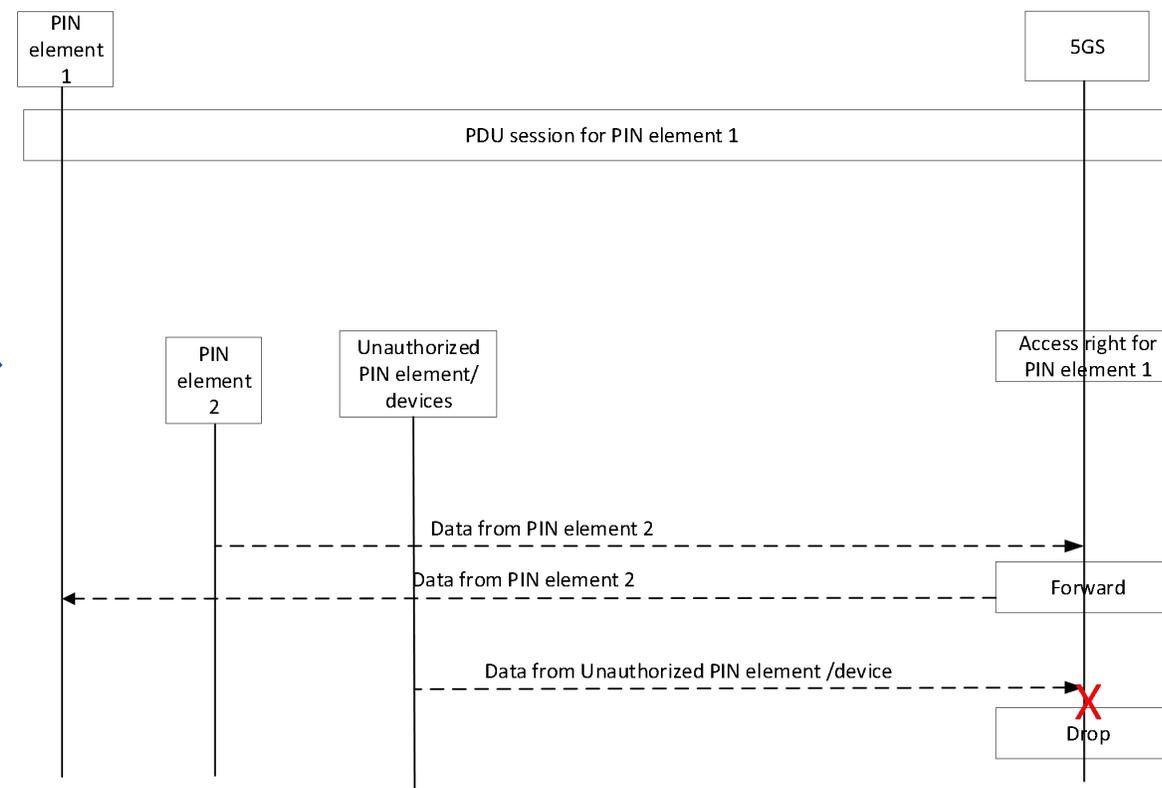
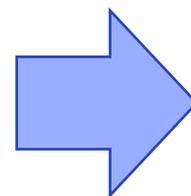
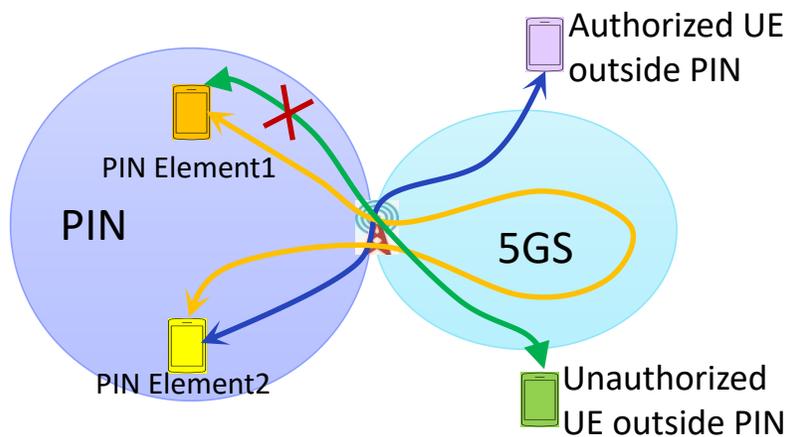
### Motivations

- Access right control over application level is not trusted, e.g., when APP server is hacked, access rules may be broken that unauthorized UE accesses the entities in the PIN or CPN network.



# Requirements from SA1

Potential high-level solution of access right enforcement for communications



# Requirements from SA1

## Policy enforcement for discovery to enable communications and/or 5GS access

- **Requirements from TS 22.261**

- 6.38.2.4 Discovery

The 5G system shall enable a UE or non-3GPP device in a CPN or PIN to discover other UEs or non-3GPP devices within the same CPN or PIN subject to access rights.

The 5G system shall efficiently support service discovery mechanisms where a UE or non-3GPP device in a CPN or PIN can discover, subject to access rights:

- availability and reachability of other entities (e.g. other UEs or non-3GPP devices) on the CPN or PIN;
- capabilities of other entities on the CPN or PIN (e.g. eRG, relay UE, connection types) and/or;
- services provided by other entities on the CPN or PIN (e.g. the entity is a printer).

The 5G system shall support a mechanism for the PIN user to indicate whether a PIN element is discoverable by other PIN elements of the same PIN.

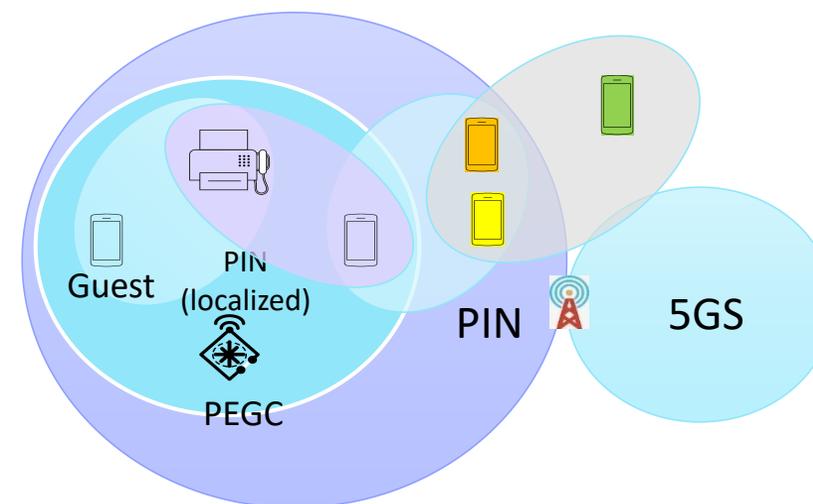
The 5G system shall support a mechanism for the PIN user to indicate whether a PIN element is discoverable by UEs that are not members of the PIN.

- **Considerations**

- E.g., entity (e.g., IP address) and service (e.g. printer) discovery in PIN/CPN to enable communications between entities (intra-communication) or external to the PIN/CPN
- E.g., capability (i.e. gateway capability) discovery to enable 5GS access.

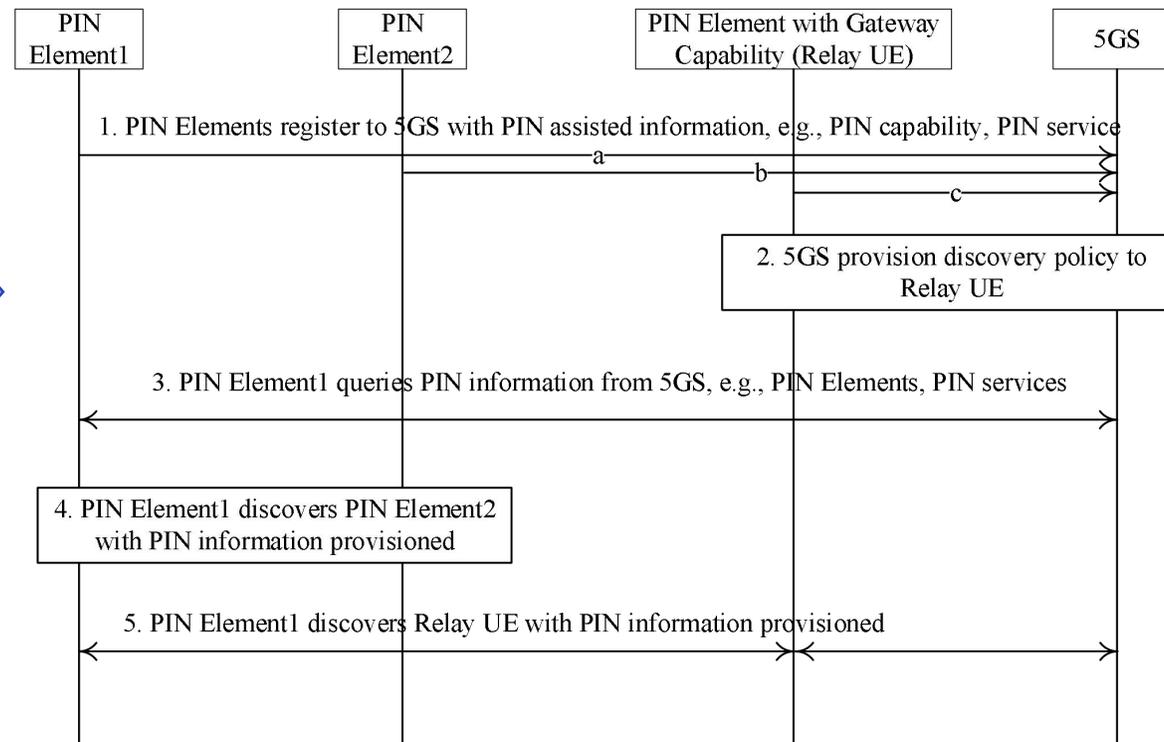
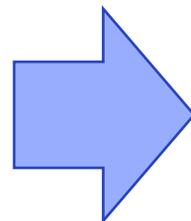
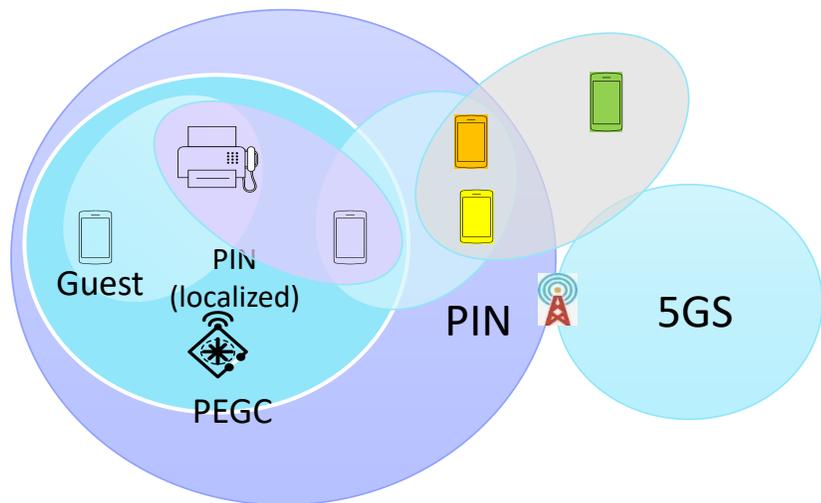
- **Motivations**

- Leverage 5GS to enforces the policy for discovery



# Requirements from SA1

Potential high-level solution of discovery (based on PC5)

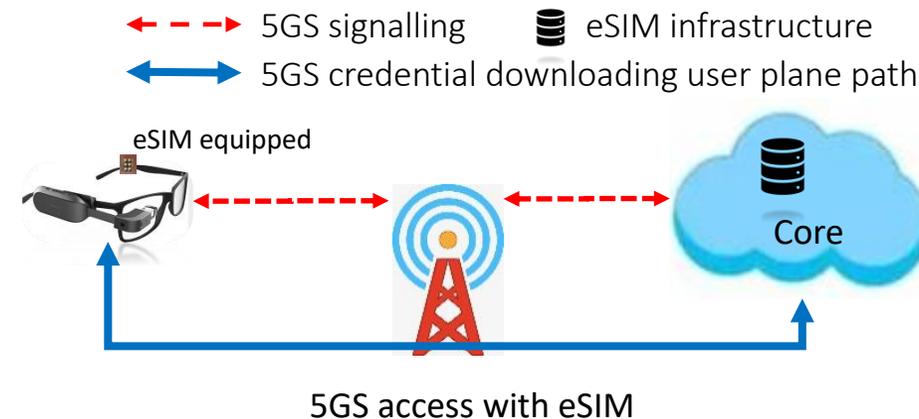


# Scenarios and Motivations

## Credential provisioning requirements



- Not suitable for devices with weight and size constraints
- Inconvenient for user to request USIM from business site
- Is not “plug and play” devices without USIM inserted



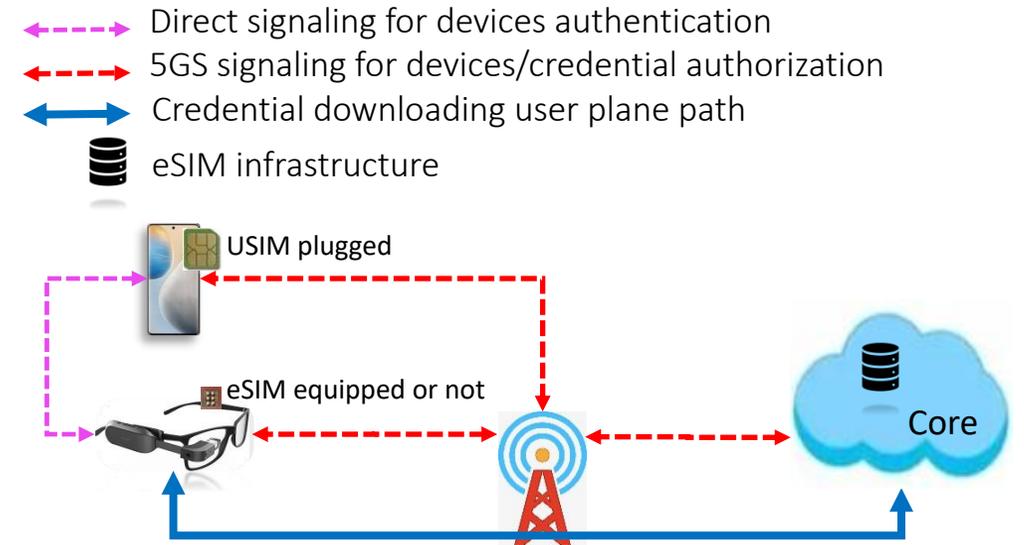
- Suitable for devices with weight and size constraints
- Not operator friendly due to home PLMN change is very easy
- No authentication/authorization before credential downloading
- Need new infrastructure for credential downloading

# Scenarios and Motivations

## Credential provisioning assisted by UE

- **Motivation:**

- Enabling devices with weight and size constraints to access 5GS, especially for those devices needs mobility and external communication
- Less impact on 5GS for credential provisioning to **affiliation devices with affiliation credential**
- E.g., Device is authenticated/authorized F2F with exchanged assisted information over PC5 (e.g. authentication via barcode scan)



Example of credential downloading **assisted by UE**

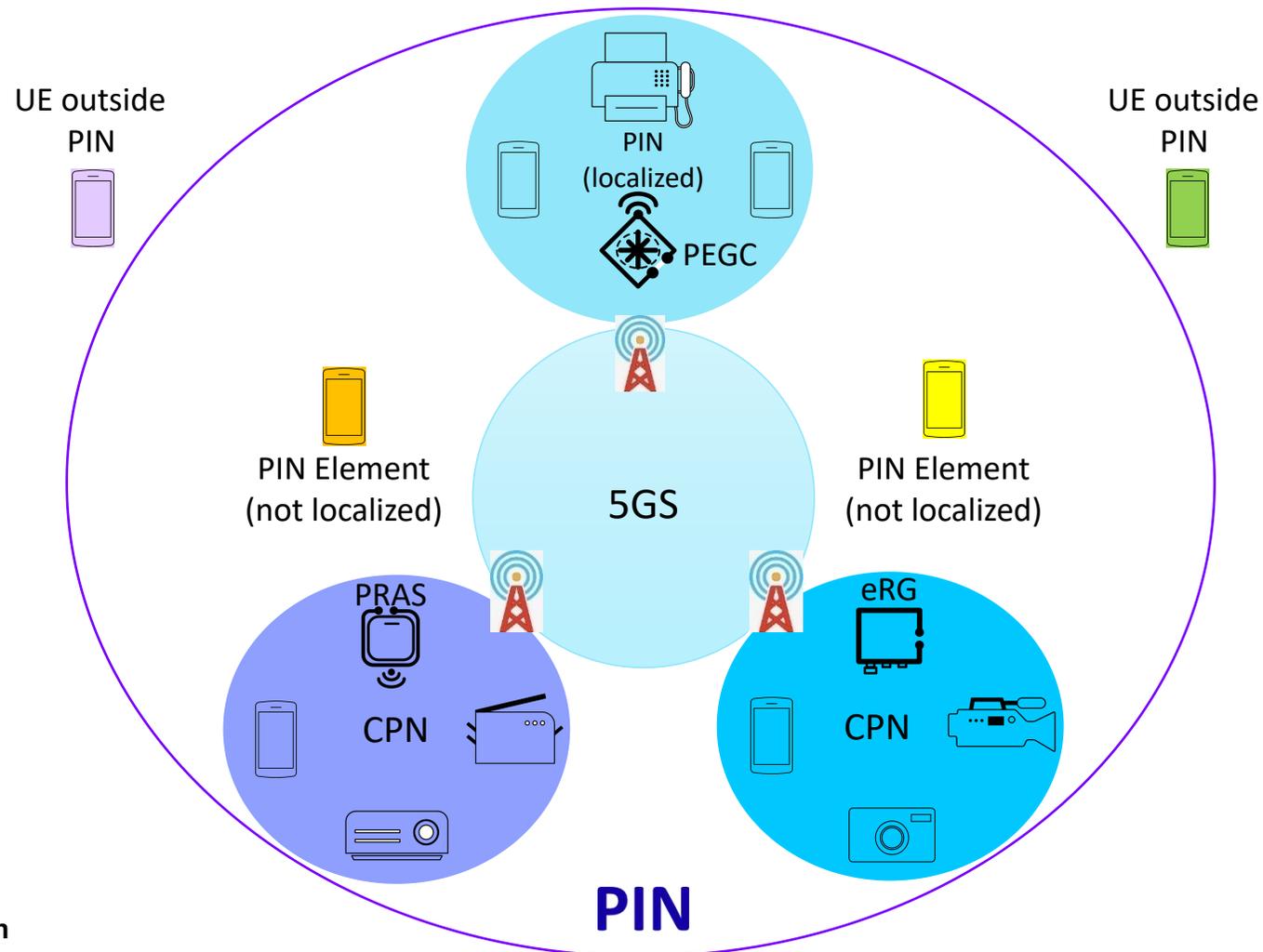
# Scenarios and Motivations

## Other possible scenarios

- **For localized PIN and CPN, the major difference is the gateway type**
  - A user may create a PIN with one or multiple following components
    - Localized PIN, e.g. at home and/or around body
    - CPN with eRG, e.g. at smart office
    - CPN with PRAS or PRAS+eRG, e.g. at smart enterprise factory
  - An entity in a PIN may request communication inside the network, which may be one of the following styles:
    - Within a localized PIN or between different localized PIN
    - Within a CPN or between different CPN
    - Between localized PIN and CPN
  - An entity in a PIN may move with one of the following styles:
    - From one localized PIN/CPN to another localized PIN/CPN
    - From localized PIN to CPN, or vice versa
    - From localized PIN/CPN to PLMN, or vice versa

**NOTE 1: CPN can be a standalone network if not managed within a context of PIN.**

**NOTE 2: PEGC is based on PC5 in Rel-18. PEGC could be PRAS or eRG in future releases.**



# CONTENTS

**01.**

Aspects

**02.**

Requirements,  
Scenarios,  
Motivations

**03.**

Objectives

**04.**

Timeline and  
work tasks