

vivo

Study on Personal IoT network (PIN)

2021.9

CONTENTS

01.

**Aspects
within PIRates**

02.

**Requirements,
Scenarios,
Motivations**

03.

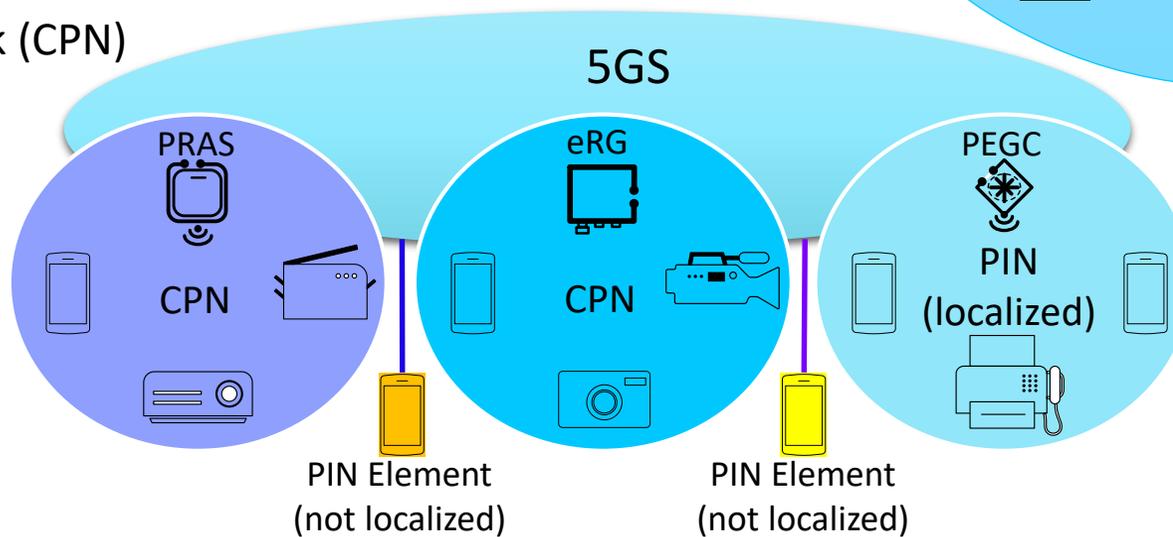
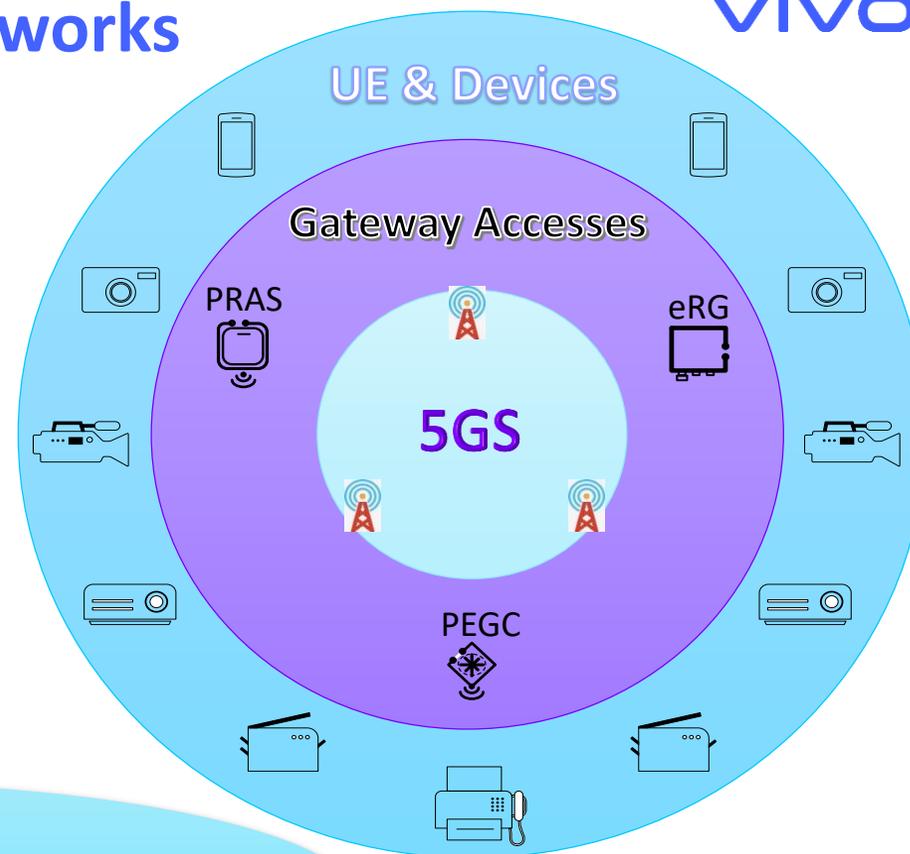
Objects

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

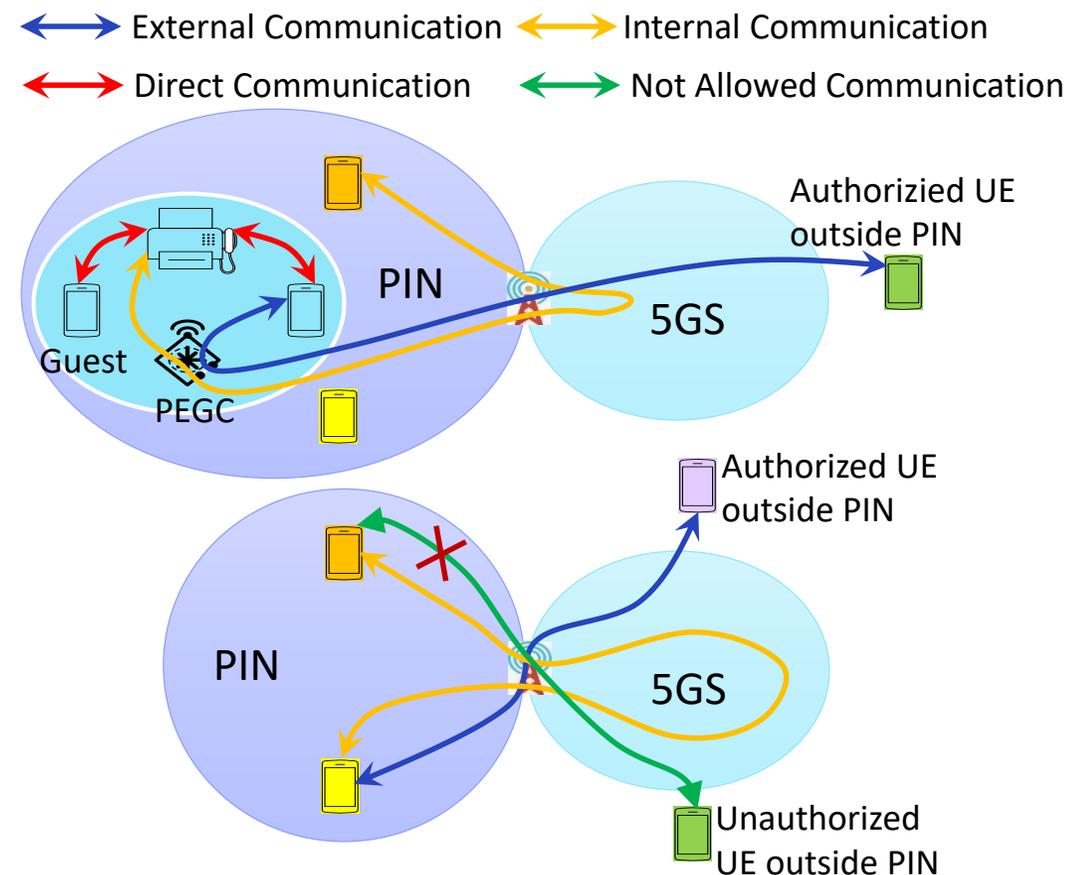
The 5G system shall support mechanisms for a PIN User, network operator or authorized 3rd party to create and manage a PIN, including:

- 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.

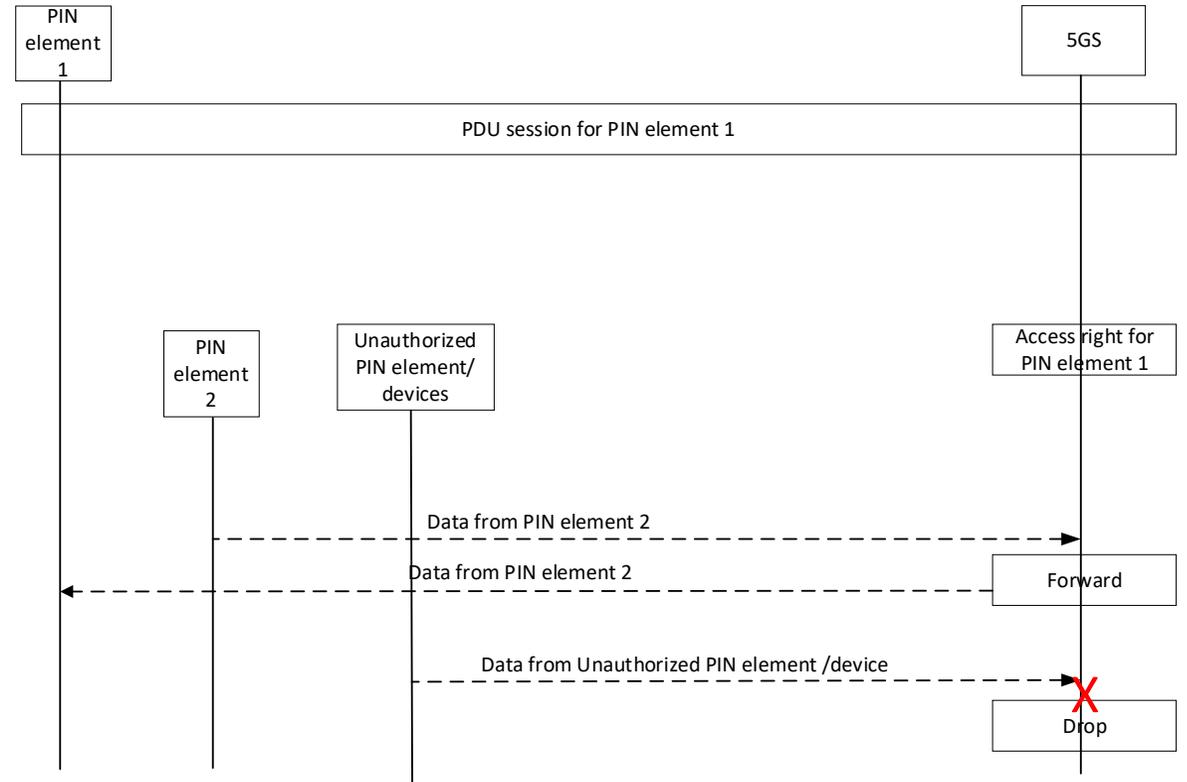
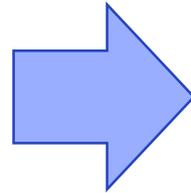
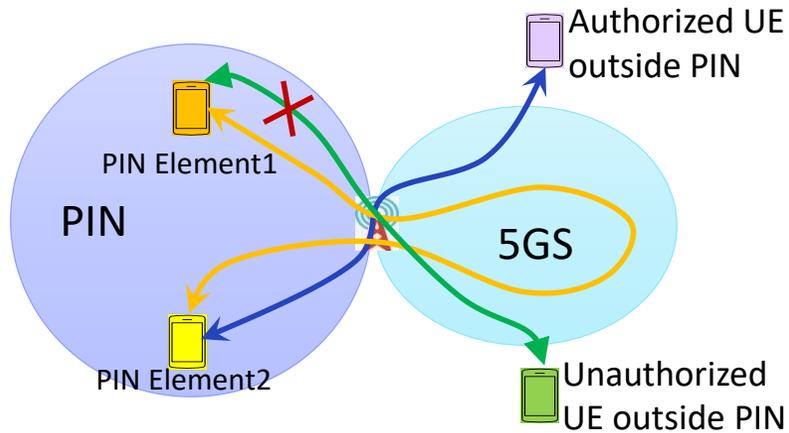
• Motivations

- 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.

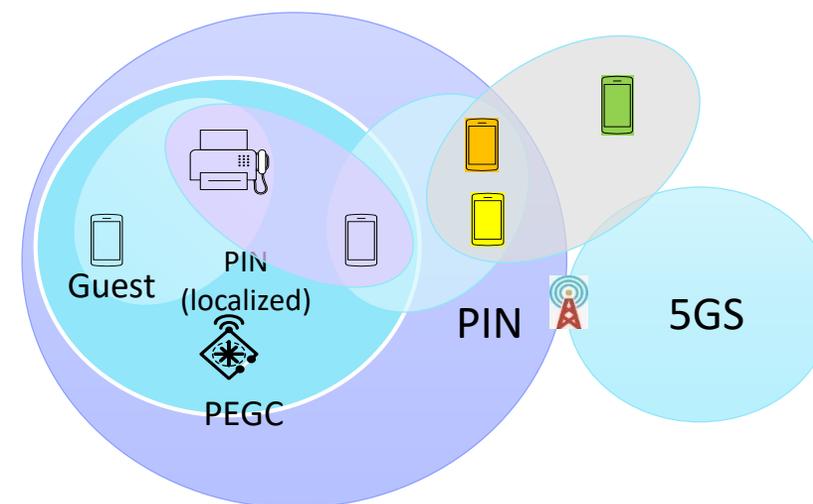
The 5G system shall support a mechanism for the PIN user to indicate whether a PIN element is discoverable by UEs that are not members of the PIN.

- **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.

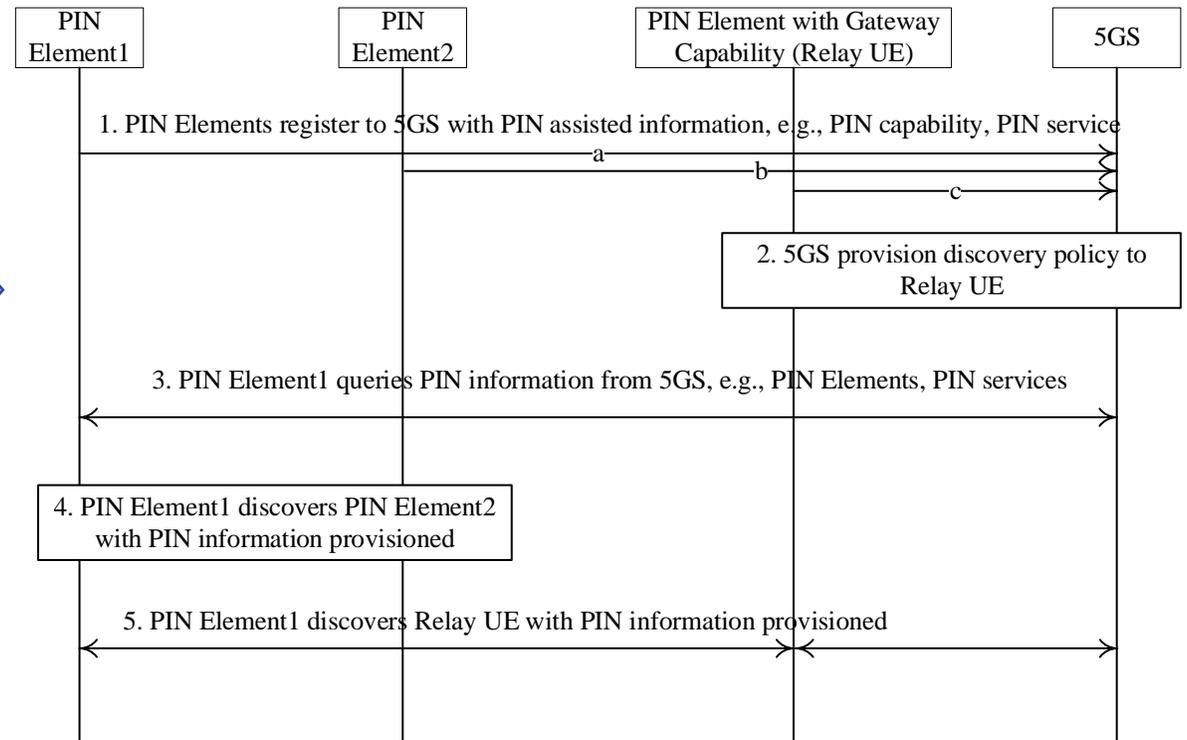
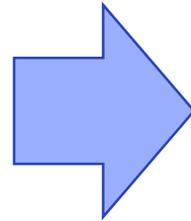
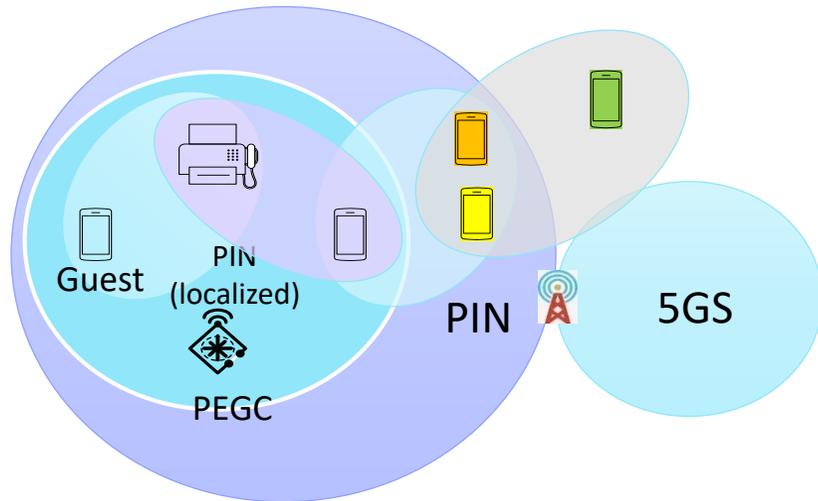
- **Motivations**

- Leverage 5GS to enforces the policy for discovery



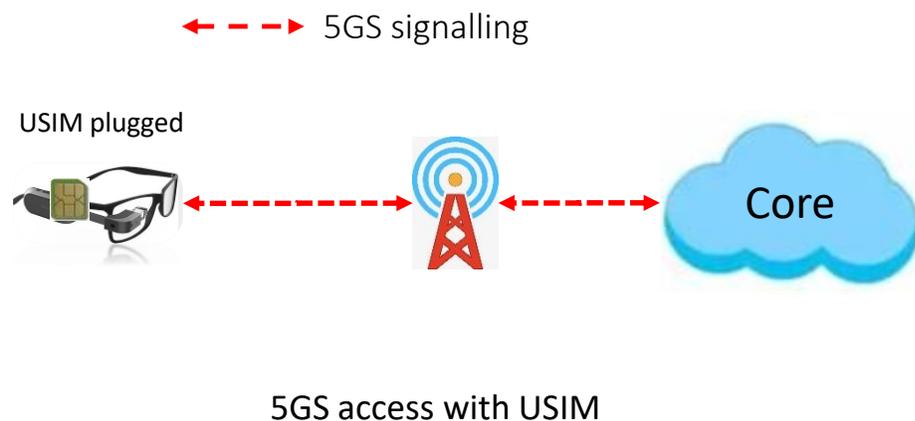
Requirements from SA1

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

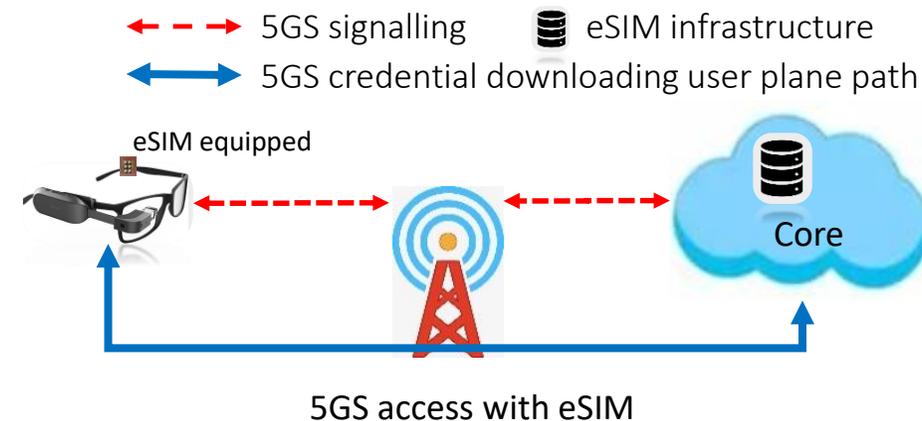


Scenarios and Motivations

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



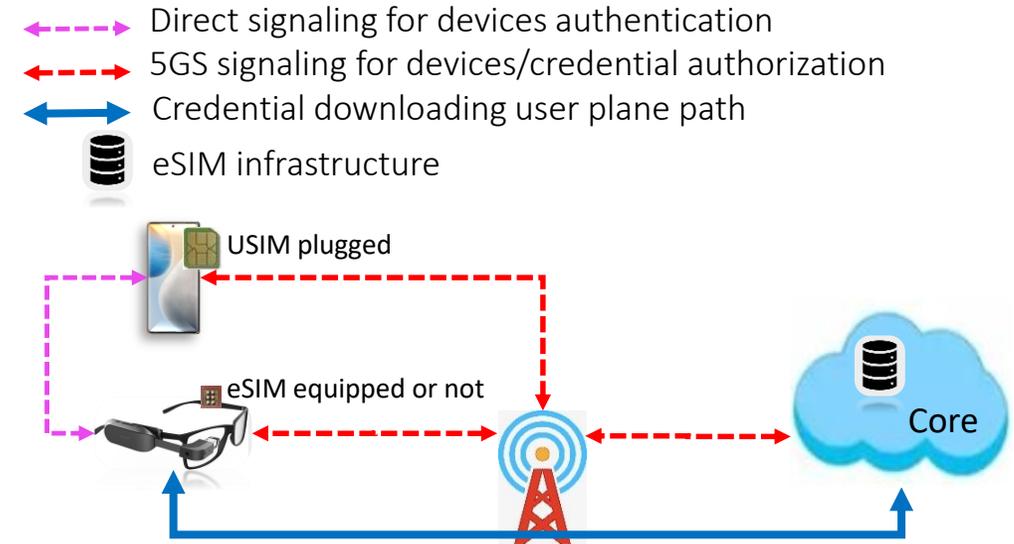
- Suitable for devices with weight and size constraints
- Not operator friend due to home PLMN change is very easy
- No authentication/authorization before credential downloading
- Need new infrastructure for credential downloading

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**

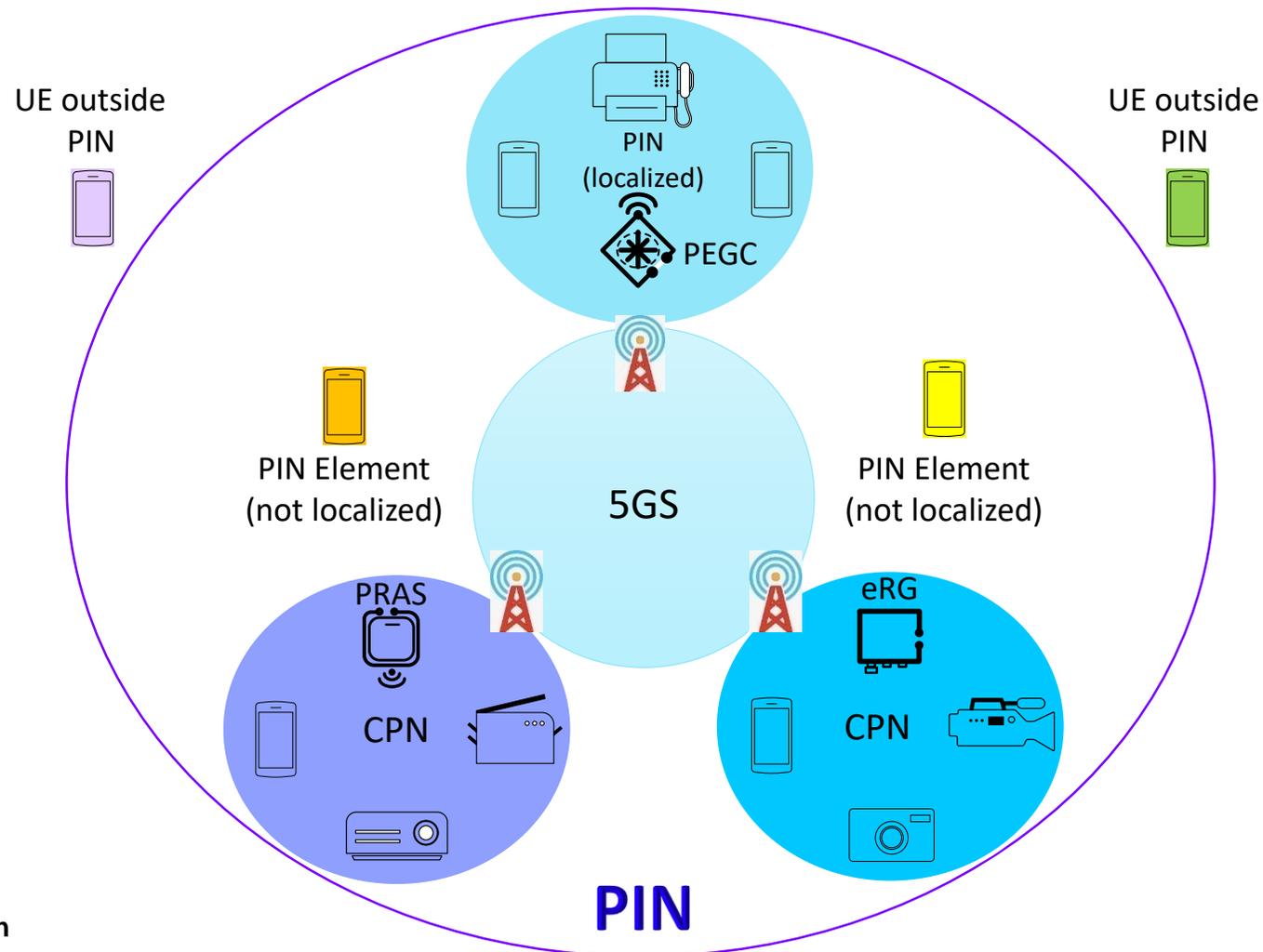
Scenarios and Motivations

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

Objectives

- Architectural enhancements to support management of PIN and access or PIN via 5GC or PEGC
- Architecture enhancements to support identifying, authenticating/authorizing, and charging in PIN
- To study the credential provisioning for PIN Elements in the PIN assisted by UEs, e.g., assisted information is provided to 5GS for credential provisioning
- To study the access right enforcement on communications
- To study the policy enforcement on network discovery, entity discovery, capability discovery, service discovery, and availability and reachability discovery
- To mitigate repeated and unauthorized attempt to access a PIN or entities in a PIN
- To study the service switch between PIN Elements within a PIN
- To study the service continuity within a PIN

CONTENTS

01.

Aspects

02.

**Requirements,
Scenarios,
Motivations**

03.

Objectives

04.

**Timeline and
work tasks**

Timeline

- Expect to start with other Rel-18 studies
 - **7 TUs for study phase and 3 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**

Work Tasks

Work Task	TUs (study)	TUs (normative)
1. Architectural enhancements to support access and management of PIN 2. Architecture enhancements to support identifying, authenticating/authorizing, and charging in PIN	(WT#1) 2	1
3. To study the access right enforcement on communications 4. To study the policy enforcement on network discovery, entity discovery, capability discovery, service discovery, and availability and reachability discovery	(WT#2) 1.5	0.5
5. To study the credential provisioning for PIN Elements in the PIN assisted by UEs, e.g., assisted information is provided to 5GS for credential provisioning 6. To mitigate repeated and unauthorized attempt to access a PIN or entities in a PIN	(WT#3) 1.5	0.5
7. To study the service switch within a PIN	(WT#4) 1	0.5
8. To study the service continuity within a PIN	(WT#5) 1	0.5

THANK YOU.

谢谢。