vivo

Study on Personal IoT networks security aspects (PIN_Sec)

2022.01

Aspects within Personal IoT Networks

- Personal IoT Networks (PIN)

  - **Wearable devices** around person, which **may be able to access 5GS directly**

  - **Smart home** with devices manufactured by multiple vendors and **may not be able to access 5GS directly**

  - **Smart office** with devices manufactured by multiple vendors and **may not be able to access 5GS directly**

  - **At least one PIN Element with Gateway Capability (PEGC) within a PIN** (c.f. 3GPP TS 22.261 clause 3.1 and 6.38.2.2)

  - Managed by PIN Element with Management Capability (**PEMC**) (c.f. 3GPP TS 22.261 clause 3.1)

  - **Non-3GPP access provided by PEGC in R18**

  - **Identities of PIN Elements are linked to 3GPP subscription of a gateway UE**

  - UE acts as device when connects to PEGC without simultaneous direct connection with 5GS

  - PEGC and PEMC are UE

  - All or part of PEGCs in a PIN may share same 3GPP subscription
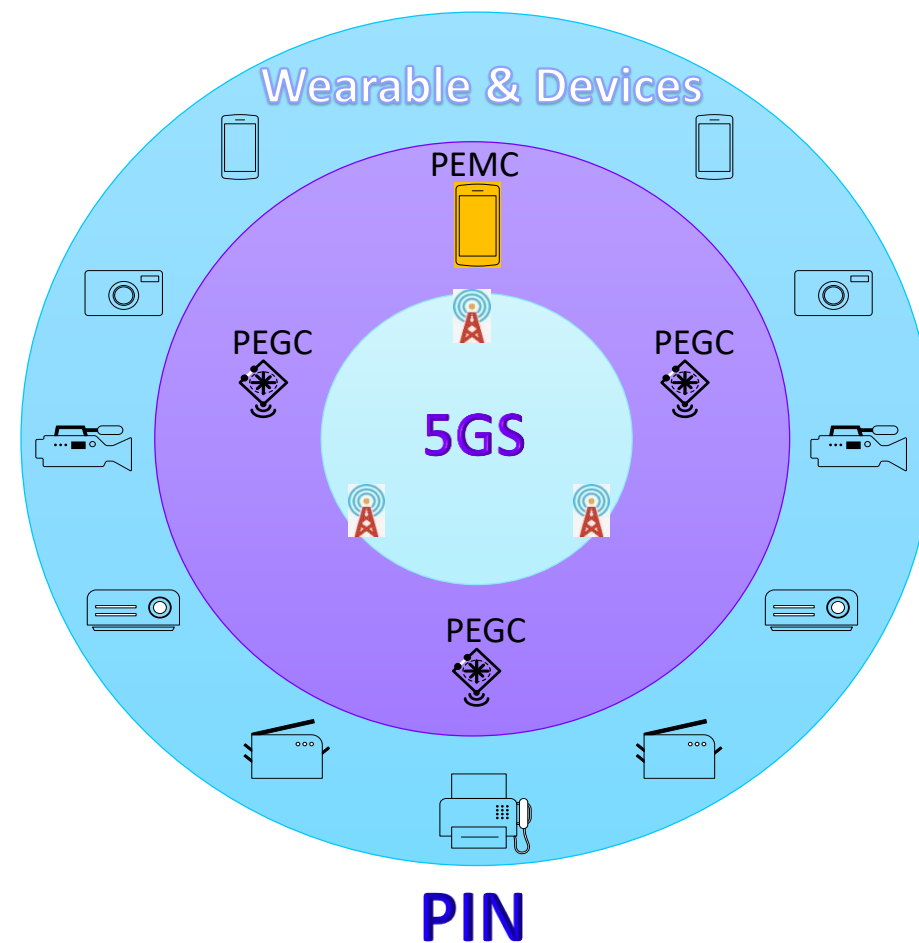
Requirements From 3GPP TS 22.101 and TS 22.261

- The 3GPP system shall support secure provisioning of credentials to a non-3GPP device connected via a gateway UE, whose user identifier has been linked with the 3GPP subscription of the gateway UE, to enable the non-3GPP device to access the network and its services according to the linked 3GPP subscription when connected via non-3GPP access. (c.f. **3GPP TS 22.101 clause 26a.2.1**)

- The 5G system shall provide user privacy, location privacy, identity protection and communication confidentiality for non-3GPP devices and UEs that are using the PIN Element with Gateway Capability, eRG or PRAS. (c.f. 3GPP **TS 22.261 clause 6.38.2.6**)

- The 5G system shall support a PIN Element using non operator managed credentials (e.g. provided by a third party) for performing communications within the PIN when those communications use PIN direct connections. (c.f. 3GPP **TS 22.261 clause 6.38.2.6**)

- The 5G system shall support a mechanism to mitigate repeated and unauthorized attempts to access PIN Elements (e.g. mitigate a malicious flood of messages). (c.f. 3GPP **TS 22.261 clause 6.38.2.6**)

Scenario – different types of device for PIN

vivo

- **Wearable device**

  - Wearable device, such as watch, glass, is able to connect to 5GS directly, but when it accesses 5GS via a PEGC, 5GC also needs to authenticate and identify it, especially when L2 relay or L3 relay with N3IWF are not supported by the device and PEGC or not deployed by operator.

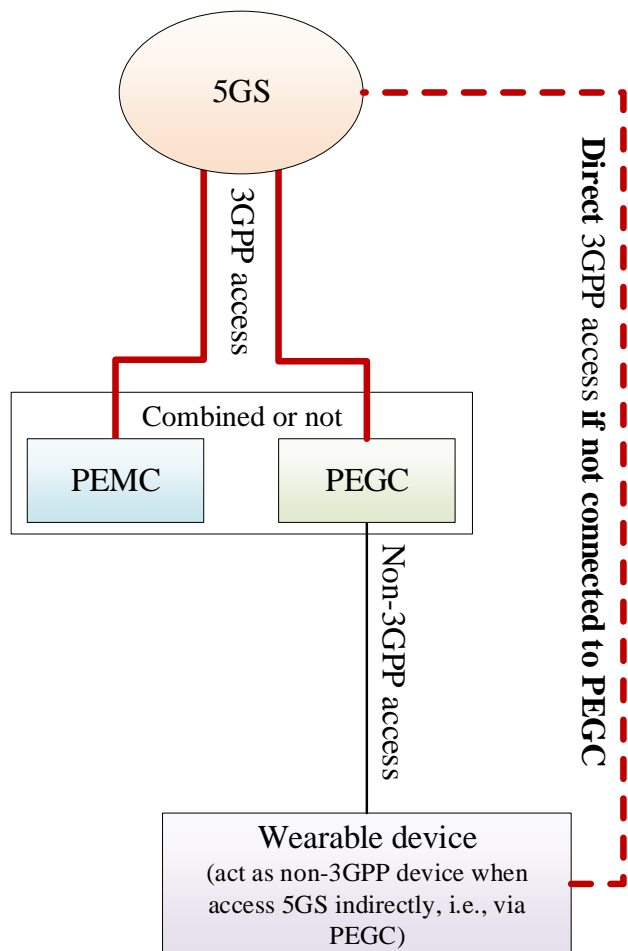- **Home/office device with 3rd party credential**

  - Home/office device may be manufactured by a vendor that deployed AAA, especially for the vendor that provides a platform for consumers to manage their devices made by the vendor. A 3rd party credential may be pre-configured in the device during manufacturing, and device support mutual authentication with the AAA, e.g., via EAP framework. This kind of device **has no capability to access 5GS directly, and may be able to be provisioned with 3GPP AKA-type credential**

- **Home/office device without credential (but pre-configured with, e.g., public keys of operators)**
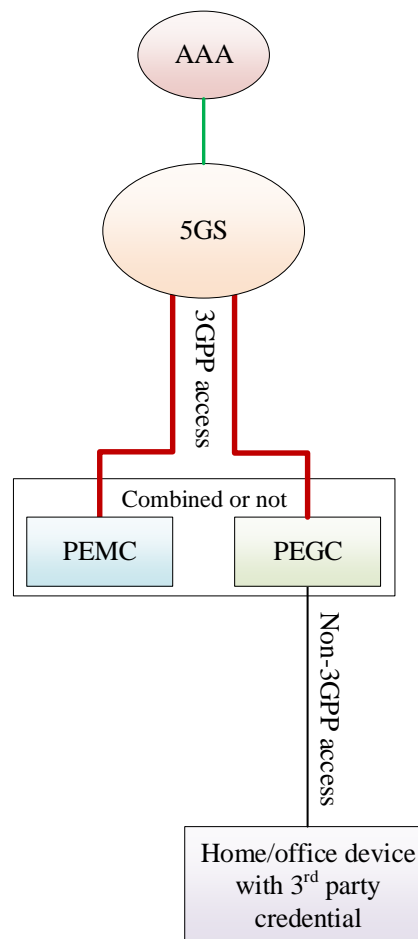
  - Home/office device may be manufactured by a vendor that does not deploy AAA, especially for the vendor that have no platform for consumers to manage their devices made by the vendor. Hence the vendor may not pre-configure credential in the device during manufacturing, but may pre-configure, e.g., public keys of operator(s), in devices. This kind of device **has no capability to access 5GS directly, and is able to be provisioned with 3GPP AKA-type credential**.
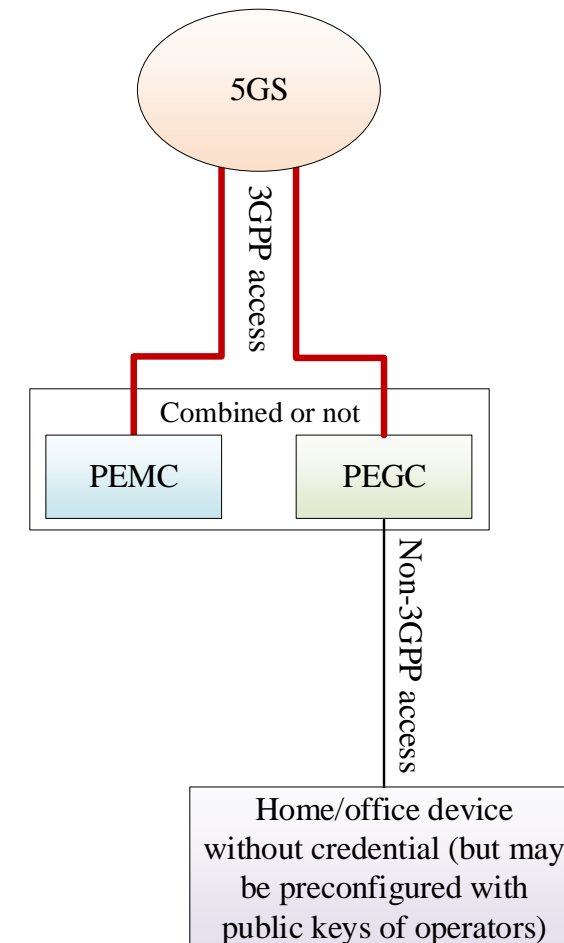
Scenario – different types of device for PIN

Wearable device

- 5GS
  - 3GPP access
  - Direct 3GPP access **if not connected to PEGC**
  - Combined or not
    - PEMC
    - PEGC
  - Non-3GPP access
  - Wearable device (act as non-3GPP device when access 5GS indirectly, i.e., via PEGC)

Home/office device (case 1)

- AAA
- 5GS
  - 3GPP access
  - Combined or not
    - PEMC
    - PEGC
  - Non-3GPP access
  - Home/office device with 3rd party credential

Home/office device (case 2)

- 5GS
  - 3GPP access
  - Combined or not
    - PEMC
    - PEGC
  - Non-3GPP access
  - Home/office device without credential (but may be preconfigured with public keys of operators)

Scenario – different types of device for PIN

- **Justification**

  - Device is able to connect to a PEGC via non-3GPP access (e.g., WiFi, Bluetooth)

  - PEGC can provide secure communication path for devices to 5GS

  - The device and the PEGC cannot automatically connect to each other when device does not have credential and the provisioning involves user interaction

  - Identifier of the credential in the device is linked to 3GPP subscription of a PEGC

  - **Device may not have direct 5GS access capability**, may not have NAS protocol

  - Device may be not allowed to be moved to another place easily

- **Motivations**

  - **Authentication:** device is able to be authenticated and identified by 5GC when access 5GS directly or via a PEGC

  - **Supporting credential provisioning:** 5GC supports credential provisioning, i.e., operator managed credential is able to be provisioned to a device via a PEGC over a secure path

  - **Authentication revocation:** 5GC is able to revoke authentication due to device mobility, e.g., from one PEGC to another, or from a PEGC to directly access 5GS or vice versa

Scenario – security protection and privacy
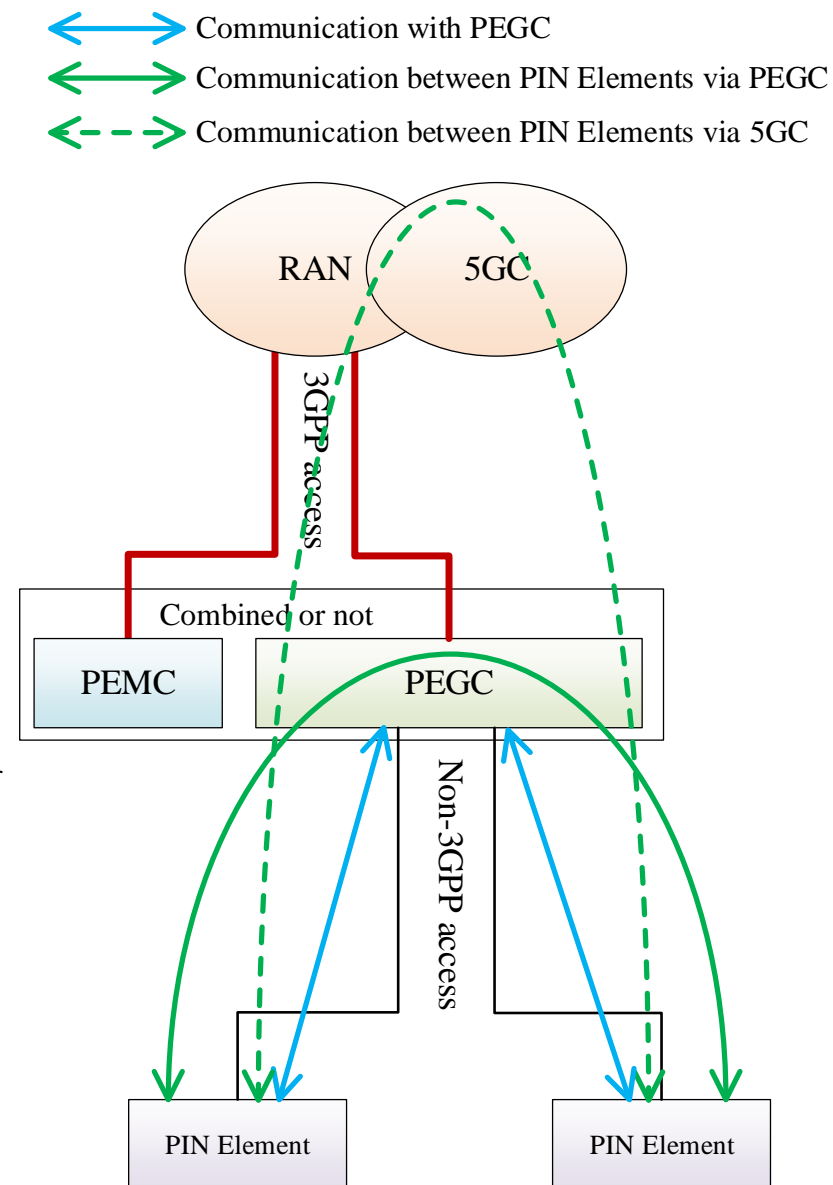
- **Gap analysis**
  - For protecting communications, both asymmetric and symmetric method can be used, but in PIN, further study is needed to, e.g., avoid MITM, mutual authenticate after PIN Elements registered into 5GS. Not all device support NAS
  - Temporary ID for PIN Elements is a way for privacy, further study is needed in PIN how to archive this
  - Barring is a method for avoiding repeat and unauthorized attempt, further study is needed in PIN to apply baring

- **Justification**
  - The communications between PIN Elements and PEGC may be required to be protected, asymmetric method may be a possible way, but how to archive mutual authentication between PIN Elements and PEGC after PIN Elements registered into 5GC is not clear
  - For communications between PIN Elements via PEGC/5GC, the two endpoints may require to be concealed from PEGC/5GC, how to avoid possible MITM is not clear
  - And there's no mechanism for using temporary IDs for PIN Elements in this study
  - How to archive mitigation of repeated and unauthorized attempts to access PIN Elements, including from internet or from other PIN Elements, is not clear

- **Motivations**
  - 5GS supports secure protection for communications between PIN Elements, e.g. via PEGC or via 5GC, or for communications between PIN Elements and PEGC
  - 5GS supports mitigation of repeated and unauthorized attempts to access PIN Elements, e.g. from internet, or from other PIN Elements via a PEGC
  - 5GS supports identity protection for PIN Elements connected to 5GS via a PEGC