**3GPP TSG-WG SA2 Meeting #157 *S2-230xxxx***

**Berlin, Germany, May 22 – 26, 2023 (revision of S2-230xxxx)**

**Source: Huawei, HiSilicon**

**Title: PIN solution principles**

**Document for: Discussion**

**Agenda Item: 9.3.2**

**Work Item / Release: PIN / Rel-18**

*Abstract: The support of PIN network requires an holistic approach to describe the overall solution which also close the gaps what has been left open by the TR. The solutions requires to be implemented in several CRs to 501/502/503 therefore the discussion paper present the global solution and the reference to related CRs*

# 1. Discussion

In next meeting we need to complete the PIN normative work and several issue remain open. In order to facilitate the discussion we present below the principles of our solution and the references to the submission documents where they are implemented in CRs:

1. **PIN ID definition and management**
   1. The External Group ID used within the 5GC is an alias of the PIN ID (seeCR A, and CR B)
   2. The Internal Group ID used within the 5GC (the Internal Group ID is mapped to the External Group ID) is sent to the UPF for traffic routing. (see CR A, and CR B)
   3. PEGCs that are part of a PIN are identified by External & Internal Group ID stored in UDR, the same as for 5G VN (see CR A, and CR B)
   4. Internal Group identifier corresponding to the PIN ID (see bullet F) is stored in the UDR (see CR C, and CR B)
   5. Internal Group identifier corresponding to the PIN ID has NAI format, where the username is the PIN ID assigned by PIN AF and the domain is the FQDN associated to the domain managing the PIN network, i.e. the FQDN of the PIN AF or of PEMC, for example [PIN\_ID\_got\_from\_AF@PIN.example.com](mailto:PIN_ID_got_from_AF@PIN.example.com). (see CR A)

NOTE: CT will decide whether the Internal Identifier for PIN is in the form of a NAI (“[PIN\_ID\_got\_from\_AF@PIN.example.com](mailto:PIN_ID_got_from_AF@PIN.example.com)”) or FQDN format (“[PIN\_ID\_got\_from\_AF.PIN.example.com](mailto:PIN_ID_got_from_AF@PIN.example.com)”) unique in PLMN. The above concept applies, with the adequate adaptations, also to the FQDN format.

1. **Who allocates PIN ID?**
   1. The PIN ID may be generated externally to 5GC by the PIN AF (see CR C and CR B) or preconfigured in 5GS.
      1. If the PIN ID is preconfigured in 5GS , e.g. a preallocated range for each 3rd party with the domain name of it, the AF and/or PEMC assigns PIN ID which is used as username. The value includes a specific username “PIN\_ID\_preconfigured @ PIN.example.com” which indicates that the PEGC belongs to a specific PIN (PIN\_ID\_preconfigured) of domain “example.com”.
   2. This mechanism is the same as for 5G VN for R18 selected solution (see CR E)
2. **PDU session (**see CR F)
   1. A PDU session can be shared by several PINs, but it **SHALL NOT BE SHARED to carry PIN and Non-PIN traffic**: if this occurs, the local switch based on 5G VN mechanism will not work properly for the PDU sessions belonging to the same PIN network.
   2. A PIN may be served by multiple PDU session in the same PEGC (e.g. when different DNN/S-NSSAI are possible for the same PIN).
   3. The PDU session dedicated to a PIN network is identified by PIN ID + DNN/S-NSSAI. The pair DNN/S-NNSAI can be the same for several PINs since the PDU session are identified via PIN ID/external Group ID which is unique.
3. **USRP**

The Internal Group ID identifying the PIN network is added to the Route Selection Components of the URSP. This will allow the matching of the rule for the PDU session supporting the PIN network.

1. **PEGC subscription & PIN management.**

The 5GS supported behaviors for PIN management (see CR A, CR G )

* 1. PIN dynamically managed
     1. Before a PEGC is assigned to a specific PIN , the Internal Group ID stored in UDM has a default value in NAI format, for example “dummy@ PIN.example.com”, or an FQDN format e.g. “dummy.PIN.example.com” to indicate that UE can act as a PEGC for PINs managed by AF of domain “example.com”.
     2. bWhen PIN ID is received by PIN AF the PIN ID\External Group ID=”PIN\_ID\_got\_from\_AF” for a UE or a group of UEs acting as PEGC (e.g. using GPSI), the 5GC verifies whether the UDM of the UE(s) includes an entry for PIN. If the entry is empty, the UE is not allowed to act as a PEGC. If the entry includes a default value (“dummy@ PIN.example.com”), the UE is allowed to act as a PEGC.   
        The 5GC stores the received PIN ID=”PIN\_ID\_got\_from\_AF”.   
        If the NAI format is used, the stored PIN ID replaces the username of the default NAI, i.e. the NAI is changed to “PIN\_ID\_got\_from\_AF @ PIN.example.com”;   
        If the FQDN is used, the stored PIN ID replaces the “dummy” portion so that the FQDN is changed to "PIN\_ID\_got\_from\_AF.PIN.example.com"   
        If the request is received by an AF not corresponding to the domain “PIN.example.com” the UE is not authorized to be a PEGC for such PIN.
     3. The initial default value can be a generic NAI such as “dummy@realm.com” to indicate that a UE can acts as a PEGC for any PIN managed by any AF.

NOTE: CT will decide whether the Internal Identifier for PIN will take the form of a NAI (“[PIN\_ID\_got\_from\_AF@PIN.example.com](mailto:PIN_ID_got_from_AF@PIN.example.com)”) or FQDN (“[PIN\_ID\_got\_from\_AF.PIN.example.com](mailto:PIN_ID_got_from_AF@PIN.example.com)”) unique in the PLMN.

The above mechanism enables the authorization of PEGCs to be part of PINs and to store the indication about which PINs the PEGC belongs to. Furthermore the PCF has the PIN information required to generate the URSP with the information required be PEGC to map the traffic to the PIN which is assigned.

* 1. PIN preconfigured in 5GS
     1. The UDM includes a specific value where the PIN ID is preconfigured via OAM, such as “PIN\_ID\_preconfigured @ PIN.example.com” which indicates that the PEGC belongs to a PIN (PIN\_ID) of domain “example.com”.

**Question to us: How to manage a PEGC which belongs to several PINs**

1. **The local switch in N6 or in UP for 5G PIN** (see R2451)
   1. A new clause is introduced to specify that local switch for PIN is based to 5G VN group mechanism with the following modifications:
      1. “PIN ID + DNN/S-NSSAI” identifies the PDU session for PIN as described in point 3. Above.
      2. The 5G VN group is used for PIN where the PDR/FAR send traffic to “internal interface” for all PDU session traffic belonging to PIN. The PDU session does not include traffic belonging to a PIN and therefore this NON-PIN traffic is not mixed with PIN and there is no need to perform additional action in order to separate it from PIN traffic.
      3. The network Instances for 5G VN local switch is associated via (PDR/FAR) to DNN/S-NSSAI + PIN ID, i.e. there is different Network Instance per each “DNN/S-NSSAI + PIN ID”
2. **PIN AF** (see S2-220xxx)
   1. The PIN AF can manage the PIN both dynamically as described in bullet 4.A or statically as described in bullet 4.B
   2. New PIN AF service separate from existing services to provision the information when a PIN is created/updated/deleted.
   3. When the PIN is created by PIN AF the PIN ID and UE ID of UE acting as a PEGC (eg. GPSI) is provided to 5GC in order to perform authorization and PIN creation (as described in bullets 4.A & 4.b)
   4. The PIN AF exchanges the information grouped as follows
      1. PIN group data
      2. PIN group membership management parameters
   5. The AF may provide QoS to be applied to PIN traffic with Nnef\_AFsessionWithQoS (see clauses 4.15.6.6 and 4.15.6.6a)
   6. The AF may provide USRP to be used with Application guidance for URSP determination (4.15.6.10) with the addition of “PIN ID + DNN/S-NSSAI” to identify the PDU session and “PIN ID” to identify the PIN network
   7. Whether the Nnef\_ServiceParameter (4.15.6.7) and Nudm\_ServiceSpecificAuthorisation (4.15.6.7a) are applicable to PIN service is FFS.
3. **PEMC role:** PEMC alone without help from the AF can only manage the Preconfigured PIN as described in bullet 4.B since the PMEC cannot communicate the PIN ID to 5GC directly. (see S2-220xxx)