

# Preventing Excessive Data Exposure within an NPN

Motivations, Use Cases and Proposal

China Telecom



The rapid digital transformation in various industries has highlighted the indispensability of wireless communication in their future. This leads to the transformation of operators' business models from 2C to 2B. To better support vertical industries with diverse requirements, NPN was introduced in Rel-16 with basic functions and has since been enhanced in subsequent releases.

3GPP supports two NPN deployments:

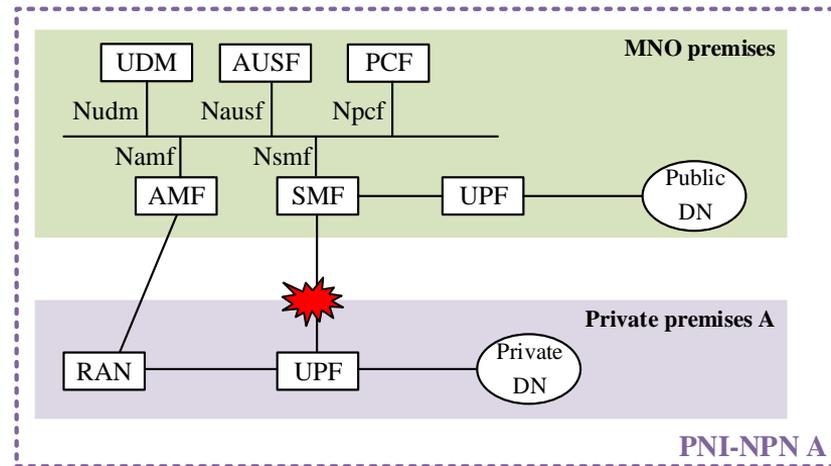
- SNPN operates independently without relying on network functions provided by a PLMN.
- **PNI-NPN is made available via a PLMN. PNI-NPN customers do not need to obtain a license for spectrum, and can reduce CAPEX and OPEX by leveraging existing public network infrastructure. In additions, operators can benefit from owning and managing UE subscription data.**

**-> PNI-NPN is a prevalent deployment option that has a low entry barrier.**

# Use Cases (1/2)

## ➤ Use case #1: sank UP and shared CP

PNI-NPN customers request the **dedicated UPF to be deployed in the private premises** (i.e. the edge of the host PLMN) for ultra-low latency communications. **All CP functions of the PNI-NPN rely on NFs deployed in the MNO premises.** The SMF in the host PLMN communicates with the dedicated UPF via N4 interface.



## ➤ Gap analysis:

Existing protection mechanisms only focus on inter-PLMN communications (e.g. SEPP), while this use case is an **intra-NPN** scenario. The dedicated UPF **physically located in the private premises and operated by PNI-NPN customers** is not always trusted by the NFs in the MNO premises, even though they **belong to one PNI-NPN**. The physical security of private premises is usually weaker than that of traditional MNO CN facilities. Moreover, if NPN customers are unable to provide a secure O&M procedure, there is a risk of **unauthorized control to the dedicated UPF by attackers**. Through anomaly operation of the dedicated UPF, attackers may obtain **sensitive information**, e.g. the topology information of NFs in the MNO premises, and utilize this information to launch attacks (e.g. DDoS attacks) on the host PLMN, **via N4**. Likewise, if the PNI-NPN is provided by a network slice, this slice contains the NFs in the MNO premises and the dedicated UPF that may not be trusted by these NFs.

## Use Cases (2/2)

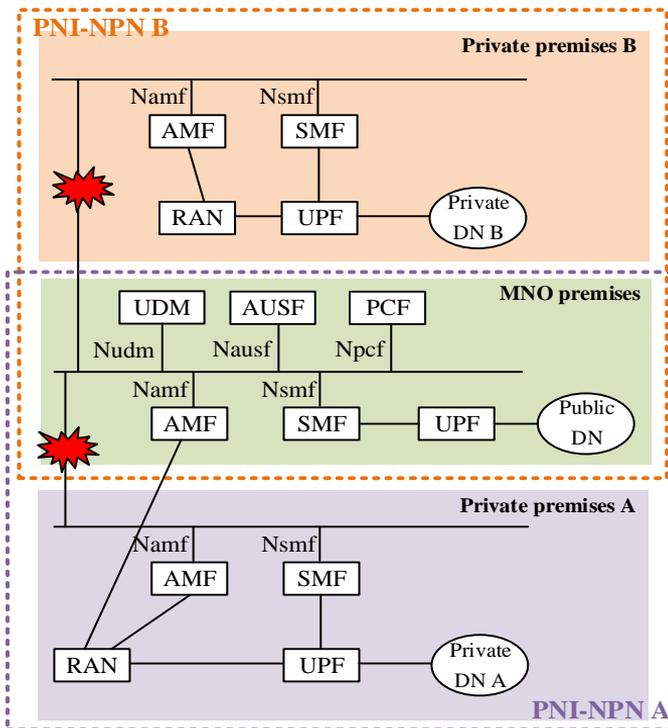
### ➤ Use case #2: sank UP and sank CP

Operators can provide the **sinking of certain CP NFs** in addition to UPF sinking. For example, to support access control with customized blacklist/whitelist, the dedicated AMF can be deployed in the private premises. Due to the highly customized and diverse nature of PNI-NPN requirements, utilizing NFs in the host PLMN leads to **excessive complexity** in operation and configuration. Moreover, successive customized requirements can result in frequent network operations that may **degrade the stability of the host PLMN**.

User authentication for multiple PNI-NPNs that are supported by the same host PLMN is performed by the shared UDM/AUSF in the host PLMN.

### ➤ Gap analysis:

Existing protection mechanisms only focus on inter-PLMN communications (e.g. SEPP), while this use case is an **intra-NPN** scenario. The dedicated NFs physically located in the private premises and operated by PNI-NPN customers are not always trusted by the NFs in the MNO premises, even though they **belong to one PNI-NPN**. Once attackers gain **unauthorized control to the dedicated NFs**, they may obtain **sensitive information** from the NFs in the host PLMN, such as the subscription/authentication data stored in the shared UDM. Attackers may also attempt to **send unauthorized service or data requests**, or generate abnormal traffic, to the shared NFs in the host PLMN. This could result in resources of these shared NFs being used to reject these dedicated NFs and thereby not be available for other NPNs hosted by the same PLMN.



This proposal aims to introduce a new service requirement for preventing excessive data exposure during the communication between two NFs within one NPN. One NF is dedicated to the NPN by sinking it into the private premises, and the other is deployed in the host PLMN and may be shared by multiple NPNs. This NPN deployment is very common for performance, security, and privacy purposes. However, the physical separation and private O&M of the dedicated NF pose a risk of excessive data exposure.

It is therefore proposed to add the following service requirement in clause 6.25 of TS 22.261:

**The 5G system shall be able to prevent excessive data exposure when a core network entity dedicated to an NPN communicates with a core network entity shared by this NPN and another network.**

**NOTE: A core network entity in an NPN can be shared by the host PLMN. It can also be shared by another NPN when the two NPNs are hosted by the same PLMN.**

# THANKS

感谢聆听

