The Standards People

Input Ike A to ETSI MEC Dario S and Walter F on 3GPP Rel 18 SNA, UP GW, PALS, CHO

Presented by:

For:

3GPP 5G
SNA
UP GW
PALS

Contents:

1. 5G Rel. 18 SNA - Subscriber-aware Northbound APIs (NAPS)

2. 5G UP GW SEPP and SeCoP (Secure Edge Protection Proxy and Service Communication Proxy)

3. 5G System PALS (Providing Access to Localized Services)

4. 5G CHO and DAPS (Conditional Handover and Dual Access Protocol Stack)

1. 5G Rel. 18 SNA - Subscriber-aware Northbound API access - 1

5G NAPS Reference model

The NEF Northbound Interface resides between the NEF and the AF.

It specifies RESTful APIs that allow the AF to access the Services and Capabilities provided by 3GPP Network Entities and securely exposed by the NEF.

An AF can get services from multiple NEFs, and an NEF can provide services to multiple AFs.

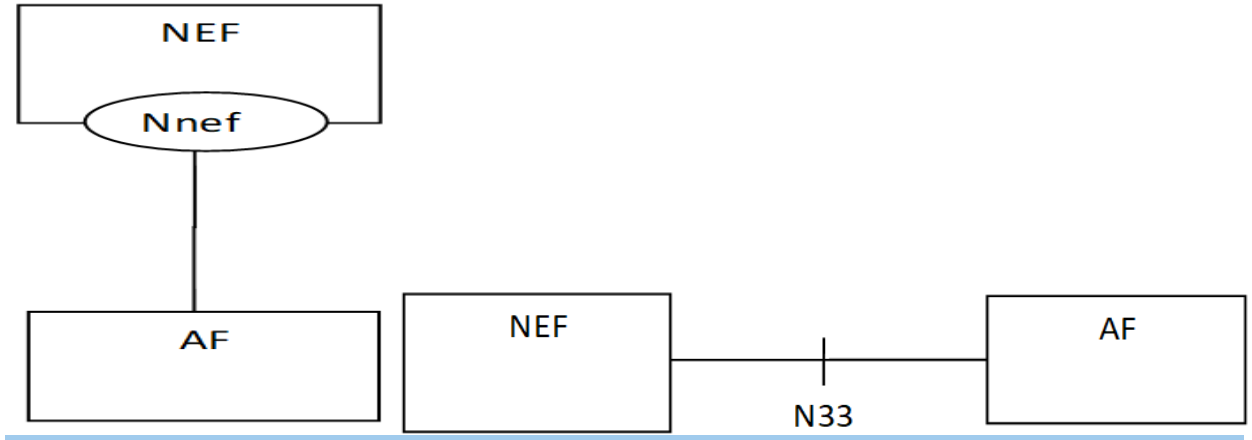

Fig. Reference Architecture for the Nnef Service SBI & Reference Point representation

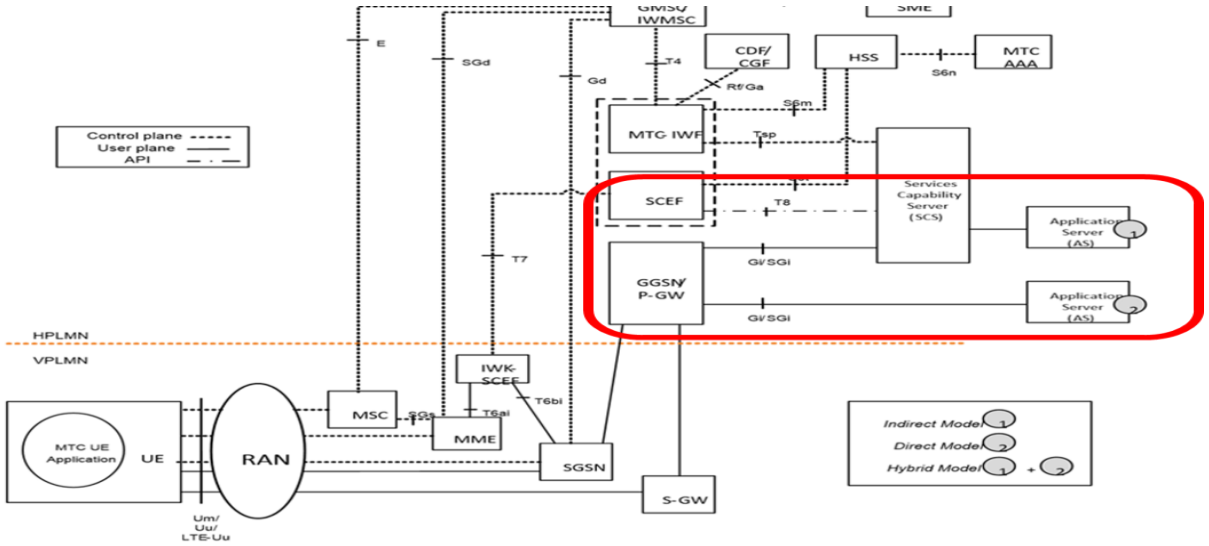

Figure 4.2-1b: 3GPP Architecture for Machine-Type Communication (Roaming)

1. 5G Rel. 18 SNA - Subscriber-aware Northbound API access - 2

3GPP 5G Rel. 18 Work Item (WI) SP - 200 797

SNA - SEES and FMSS NAPS to 5G Subscribers in MNO

"The Operator shall be able to provide to a 3rd Party Service Provider secure and chargeable access to the Exposed Services/Capabilities i.e. to Authenticate, Authorize and Charge the 3rd Party entities."

MNO can allow the API access of a 3rd Party Entity (ISP/ICP) by taking into account the 5GS Subscriber-based check.

Possibility of utilizing those APIs can be open directly to the 5GS Subscriber.

MNOs need to be cautious of securing its 5GS Subscribers' Privacy.

3GPP TSG SA Meeting # 89e SP-200797
Electronic Meeting, September 15th – 21st 2020

Source: SA1 (from S1-203296)
Title: New WID on Subscriber-aware Northbound API access (SNA)
Document for: Approval
Agenda Item: 6.6

3GPP™ Work Item Description

Information on Work Items can be found at http://www.3gpp.org/Work-Items
See also the 3GPP Working Procedures, article 39 and the TSG Working Methods in 3GPP TR 21.900

Title: Subscriber-aware Northbound API access

Acronym: SNA

Unique identifier: 890024

Potential target Release: Rel-18

Note that this field above indicates the proposed Release at the time of submission of the WID to TSG approval. It can later be changed without a need to revise the WID. The updated target Release is indicated in the Work Plan.

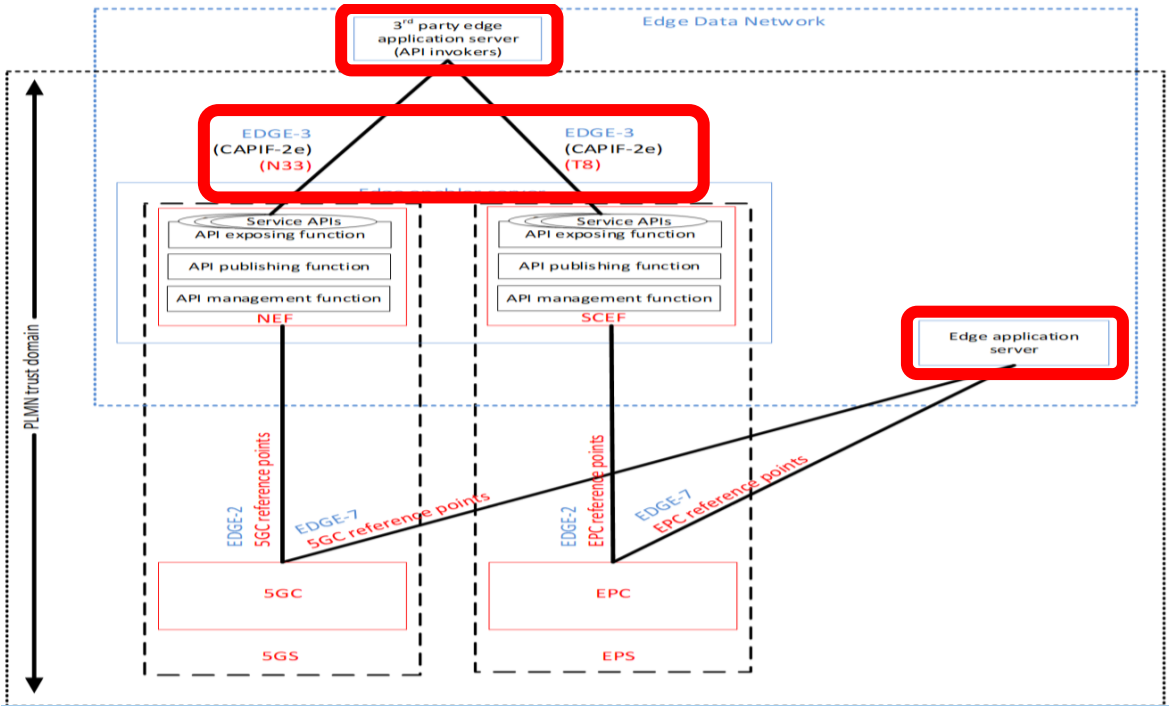

Figure 7.10.1.4.-1: EES and EAS direct interaction with 3GPP Core Network

2. 5G UP GW SEPP (Secure Edge Protection Proxy) - 1

Solution #20: UP Gateway (GW) Function on the inter - PLMN N9 interface

This solution provides a solution for Key Issue #27.

The SEPP-U is a GW Function used for filtering GTP-U traffic on the N9 interface.

The SEPP-U filters GTP-U messages in a way that only genuine GTP-U packets, that correspond to active PDU sessions established through the N32 interface, can transit through the GW. All other GTP-U packets are discarded and logged. This ensures that no unwanted GTP-U packets enter or leave the Mobile Network.

The SEPP-U Function may be deployed either at the Edge of the Operator Network or collocated with the UPF. It monitors incoming/outgoing GTP-U traffic on the N9 Interface and executes GTP-U checks on every GTP-U packet on the N9 Interface.

SEPP-U interacts with SMF over the Nx Interface to obtain Local and Remote TunnelInfo Information **(TEID and tunnel IP address**).

SEPP-U operates as a transparent GW, which sits on the IP Route, examines each Packet and decides to either pass it or drop it.

In the following figure, SEPP-U is shown as a separate function in front of UPF to only forward GTP-U traffic, belonging to successfully established PDU sessions.

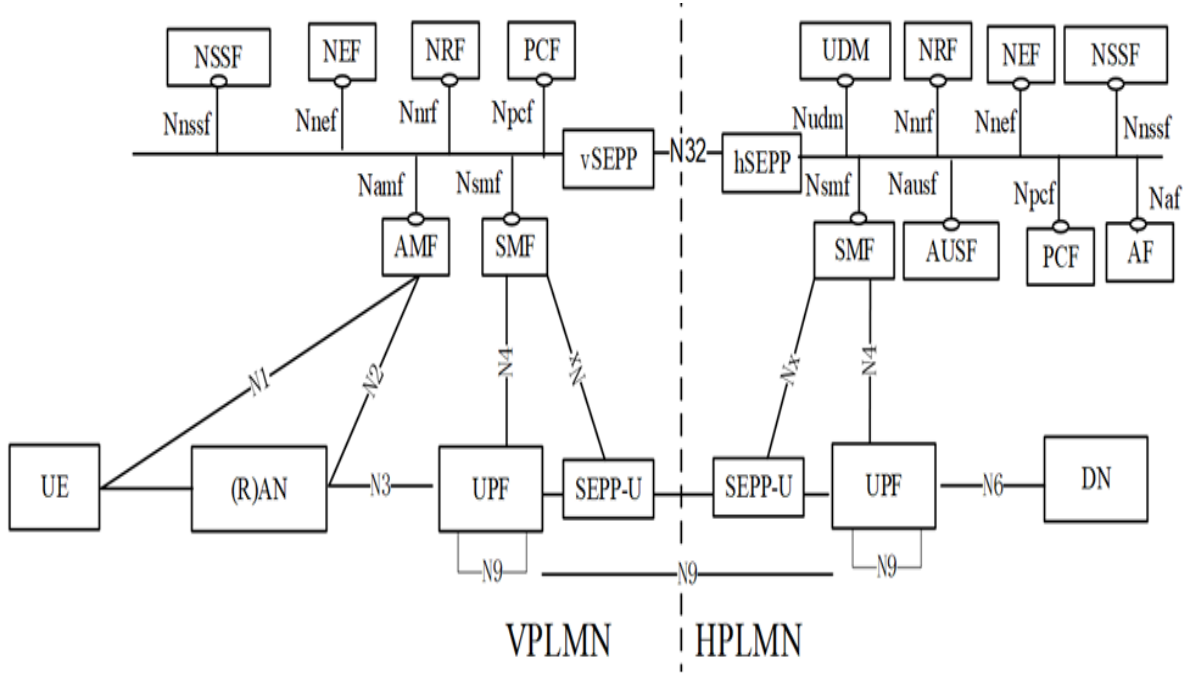

Fig.: UP GW Function SEPP (Secure Edge Protection Proxy) for the inter - PLMN N9 Interface

2. 5G UP GW SEPP and SeCoP - 2

Solution Key Issue #27: Policy based Authorization for Indirect Communication between Network Functions (NFs)

This solution addresses KI #22 - Authorization of NF Service Access in Indirect Communication.

The solution proposes Policy-based Authorization of NF Consumer requests in the SeCoP (*Service Communication Proxy)* associated with the NF Producer.

A Set of Policies are provisioned in the SeCoP which allow the SeCoP to recognise an incoming Service Request from a NF Consumer and determine whether to allow the request and set of services that can be allowed for the requesting NF.

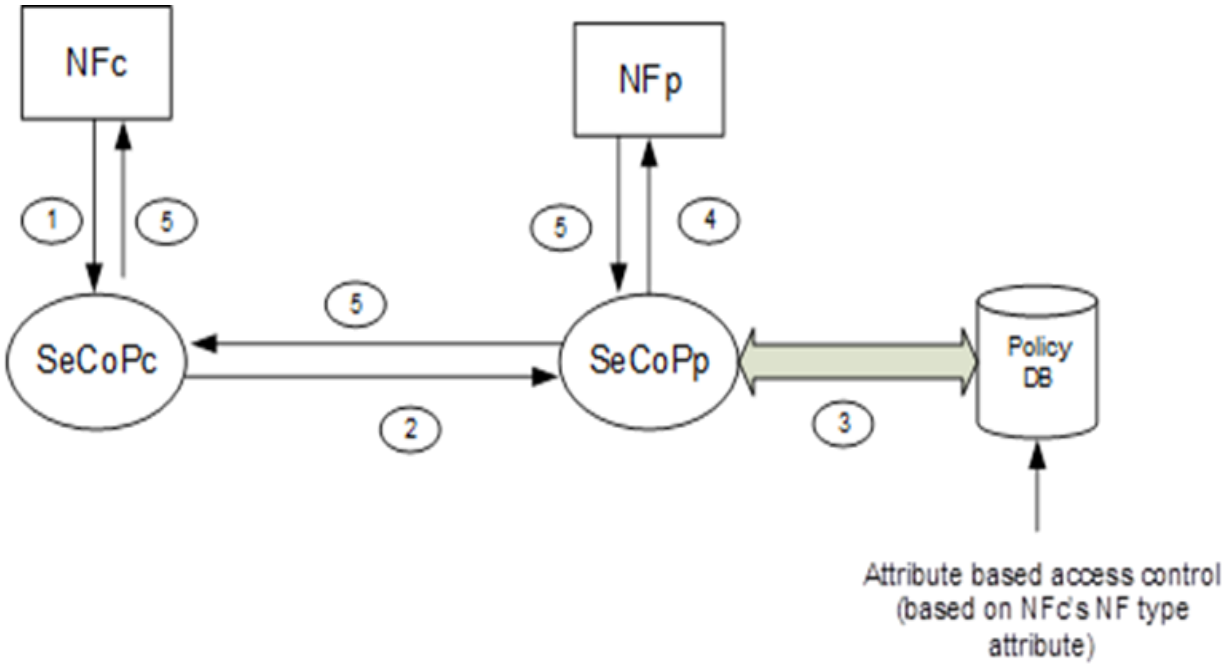

Fig.: Policy based Service Access authorization of NF consumer

3. 5G System PALS -Providing Access to Localized Services - 1

Business Model for Providing Access to Localized Services (PALS)

Key Partners include: Network Operators (MNOs, NPN Operators, Fixed Operators, etc.), Local Service Providers, Individuals (Users), Owners of Facilities or Proprietors of Business in which the Local Access will occur and 3rd Party Service Providers. These stakeholders will work together to provide Local Access to Services.

The main activities are related to how to Commission and Decommission Access, as including the relevant Services.

The Access is not merely to a *Network*, but to a Set of *Services* offered by Local Service Providers, the Network Operator and 3rd Parties.

Since the access is *local* and may be bounded in time and space, the effort to de/commission accesses and services will have to be very light-weight (not requiring lots of lead-time, complexity, in-person consulting and customization, etc.)

Secondly, from a user perspective, the user must become aware of access and local services, to choose to access them. The process by which the user and their equipment gain access to the network, use it and terminate access (and service) will be efficient, simple and result in a user experience that seems convenient and to offer resources and services that cannot be accessed any other way.

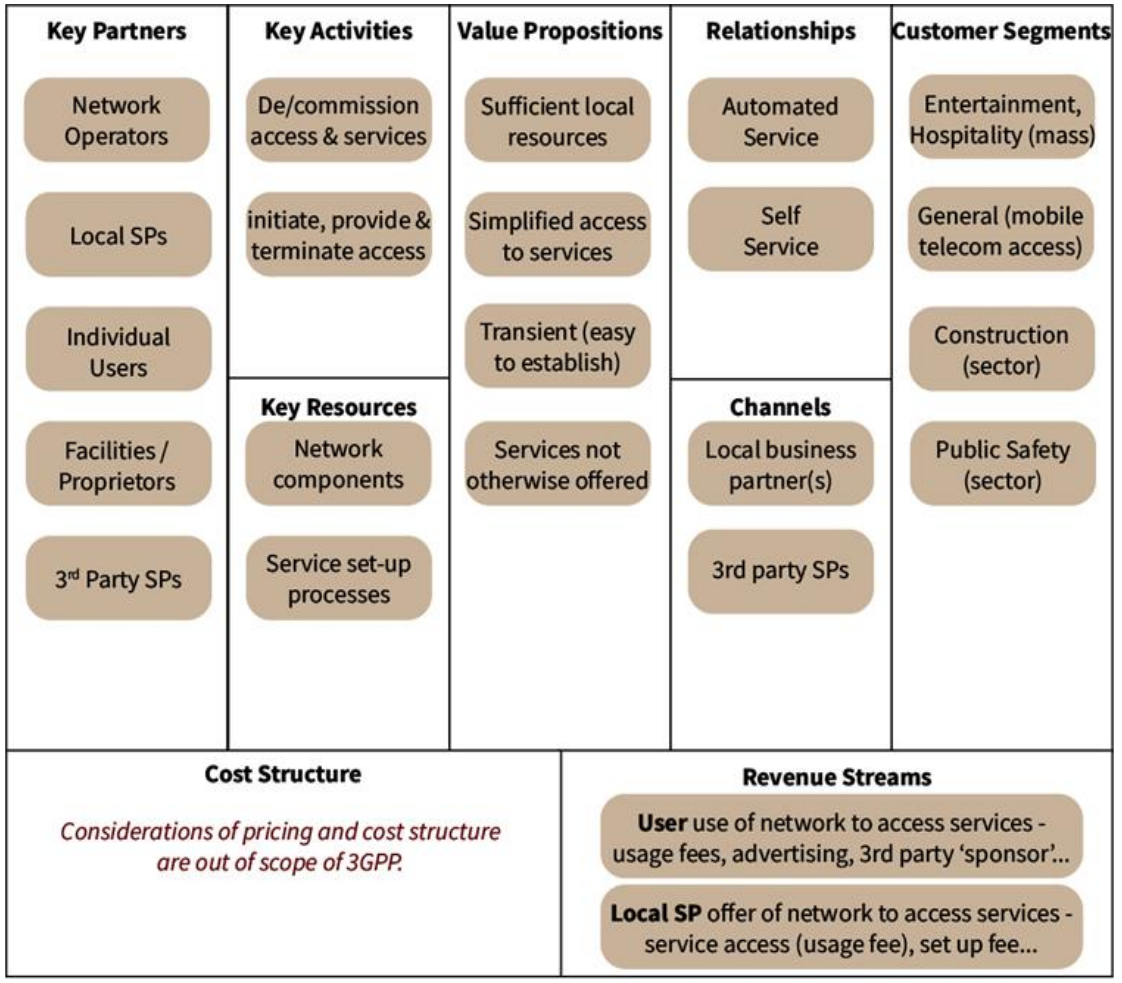

Fig.: A 5G Business Model Canvas for Providing Access to Local Services

3. 5G System PALS -Providing Access to Localized Services - 2

Interworking between Networks Operators (NOs) & Application Providers (APs) for Localized Services Roaming Scenarios applicable for interworking between Hosting Network Operator (PLMN or NPN) and Data Applications based on Service Agreements for Localized Services among Network Operators & Application/Service Providers:

- Hosting Network Operator owns the 5G Network which provides Access and IP Connectivity to Roaming UEs.
- Network Operator owned Application Layer entities include Service Hosting Environment, and IMS Network.
- Application Platforms in 3rd Party Domain can be owned by 3rd Party Application/Service Providers, or Home/other Network Operators.
- The Application Platforms could be Application Servers (e.g. Video on Demand Server, Cloud Gaming Server, etc.), 3rd Party SW Development Platforms, & 3rd Party/Operator Service Hosting Environments.

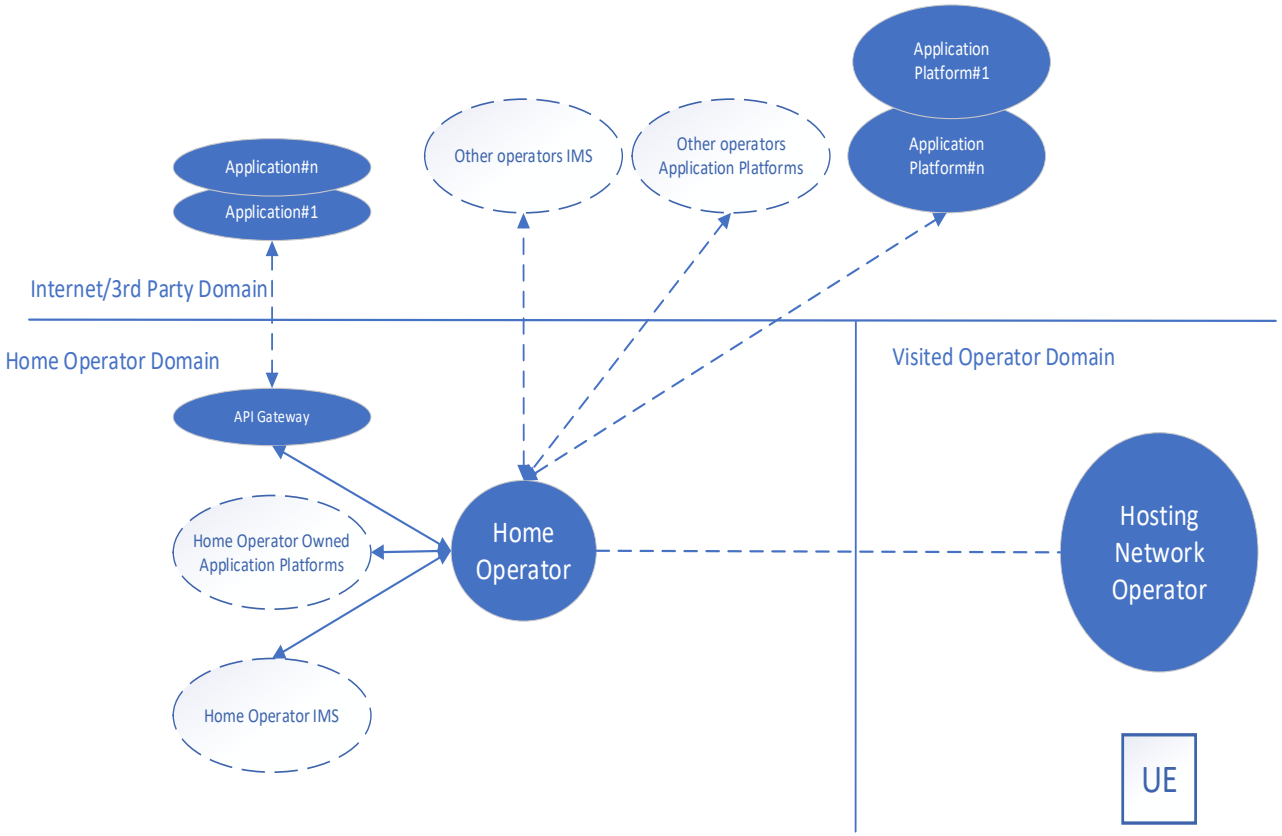

Fig.: Home Operator owned/collaborative Roaming Scenario - Home Routed

3. 5G System PALS -Providing Access to Localized Services - 3

The Figure provides the Local Breakout Scenario for both owned and collaborative scenarios between Visited Hosting Network Operator and Operators in 3rd Party Domains where Traffic is routed to Application from the Hosting Network to:

1) Hosting Network owned Application Platforms,

2) Collaborative Home Network owned Application Platforms,

3) 3rd Parties via Roaming Agreements between Visited Hosting Network Operator and Home/Other Network Operators, and between Hosting Network Operators and other Application/Service Providers.

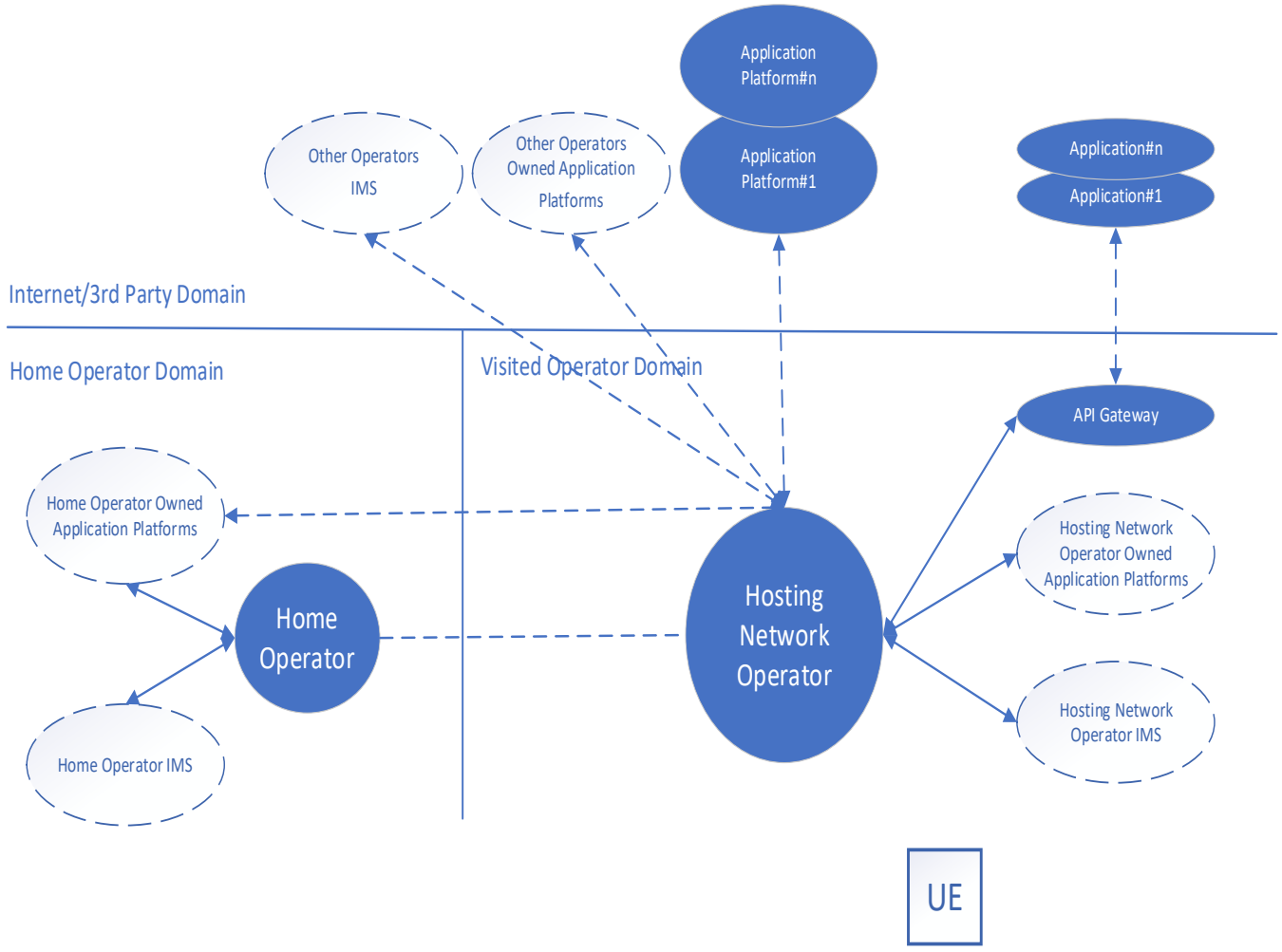

Fig.: Hosting Network Operator owned/collaborative Roaming Scenario – Local Breakout

4. 5G System CHO and DAPS - 1

Conditional Reconfiguration

The Network configures the UE with one (1) or more Candidate Target SpCells in the Conditional Reconfiguration.

The UE evaluates the condition of each configured candidate target SpCell.

The UE applies the conditional reconfiguration associated with one (1) of the target SpCells which fulfils associated execution condition. The Network provides the configuration parameters for the target SpCell in the *ConditionalReconfiguration* IE.

A **Conditional Handover (CHO)** is defined as a handover that is executed by the UE when one (1) or more Handover execution conditions are met. The UE starts evaluating the execution condition(s) upon receiving the CHO Configuration, and stops evaluating the execution condition(s) once a Handover is executed (Legacy Handover or Conditional Handover execution).

The CHO Configuration contains the Configuration of CHO Candidate Cell(s) generated by the candidate gNB(s) and execution condition(s) generated by the source gNB.

- An execution condition may consist of one (1) or two (2) trigger condition(s) (CHO events A3/A5, as defined in [12]). Only single RS type is supported and at most two different trigger quantities (e.g. RSRP and RSRQ, RSRP and SINR, etc.) can be configured simultaneously for the evaluation of CHO execution condition of a single candidate cell.
- Before any CHO execution condition is satisfied, upon reception of HO command (without CHO configuration), the UE executes the HO procedure as described in clause 9.2.3.2, regardless of any previously received CHO configuration.
- While executing CHO, i.e. from the time when the UE starts synchronization with target cell, UE does not monitor source cell.

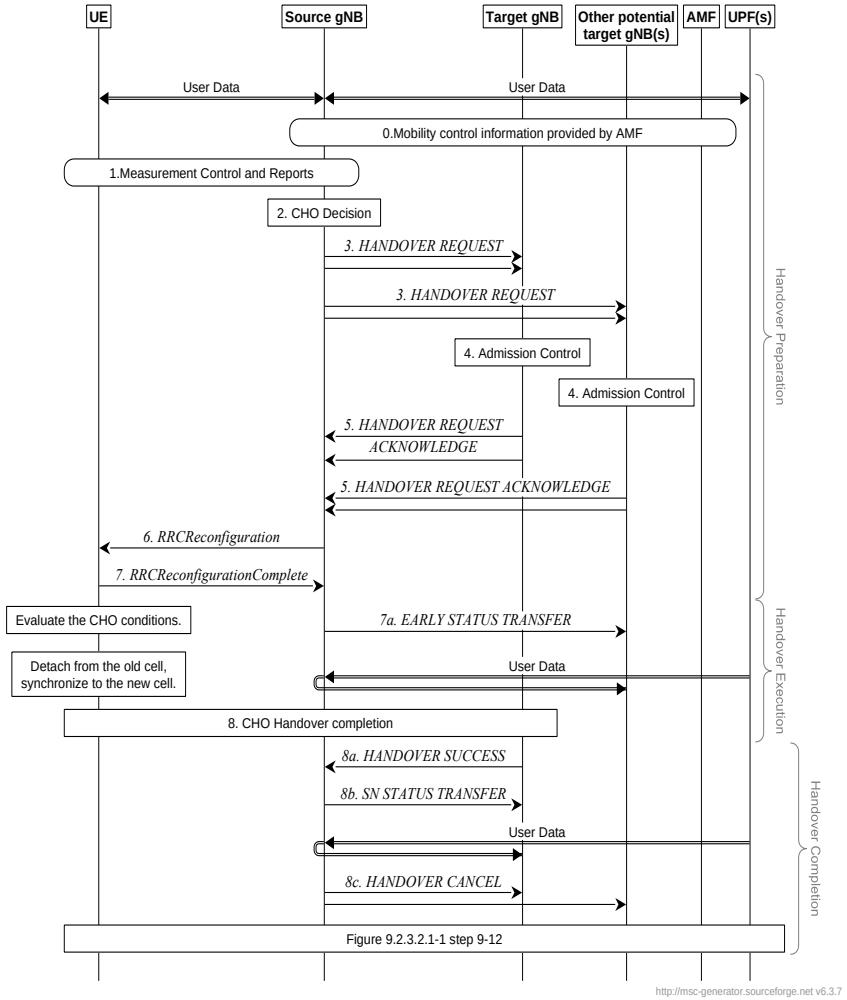

Fig.: Intra-AMF/UPF Conditional Handover

4. 5G System CHO and DAPS - 2

Conditional Reconfiguration

The Network configures the UE with one (1) or more Candidate Target SpCells in the Conditional Reconfiguration.

The UE evaluates the condition of each configured candidate target SpCell.

The UE applies the conditional reconfiguration associated with one (1) of the target SpCells which fulfils associated execution condition. The Network provides the configuration parameters for the target SpCell in the *ConditionalReconfiguration* IE.

DAPS - Dual Access Protocol Stack

The main characteristics of the Reduced Mobility Interruption Solution are:

- Continued transmission/reception in the Source Cell after receiving the Handover Request
- Simultaneous Reception of User Data from Source and Target Cell
- Uplink Transmission of User Data switched to Target Cell at completion of Random Access Procedure

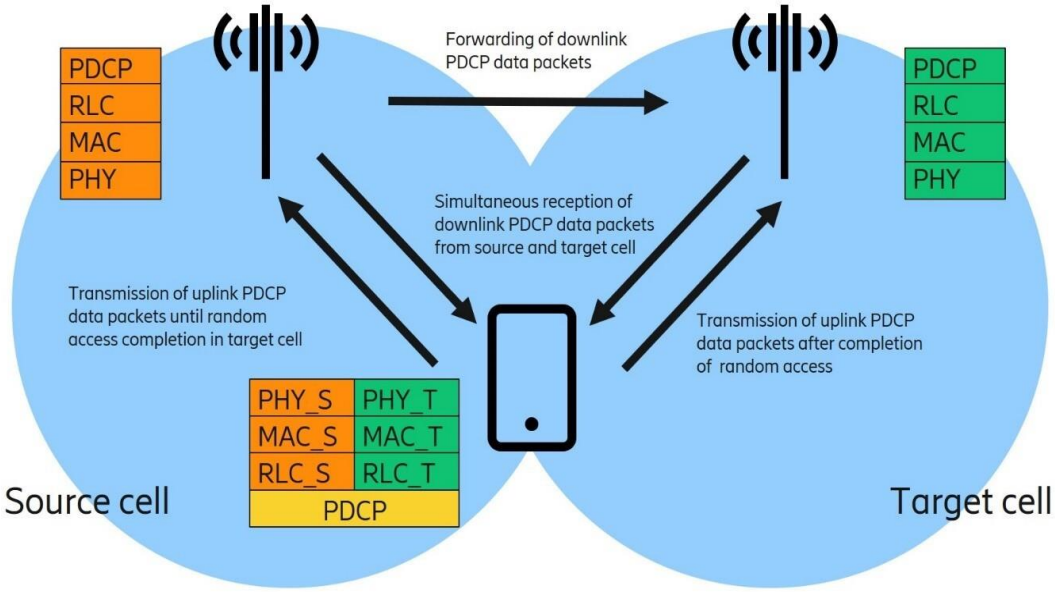

Fig.: An overview of the proposed 3GPP Solution for Reduced Handover Interruption Time - **Dual Active Protocol Stack (DAPS) handover**

Upon receiving the Request to Perform a Handover with reduced interruption time, the Mobile Terminal continues to send and receive User Data in the Source Cell. At the same time, a new connection to the Target Cell is established and the Mobile Terminal performs synchronization and Random Access in the Target Cell. The Mobile Terminal will establish a New User Plane (UP) Protocol Stack for the Target Cell, containing PHY (Physical), MAC (Medium Access Control) and RLC (Radio Link Control) layers, while keeping the Source User Plane (UP) Protocol Stack active for transmission and reception of User Data in the Source Cell.