**3GPP TSG SA WG 1 Meeting #99e S1-** **222020**

**Electronic Meeting, 22 August – 1 September 2022** *(revision of S1-221100)*

**Source: CATT, China Unicom**

**pCR Title: Pseudo-CR on use case of flexibility and security for non-N2 sharing network**

**Draft Spec: 3GPP TR 22.851 v0.1.0**

**Agenda item: 7.5**

**Document for: Approval**

**Contact: Wan Qing** **wanqing1@cictmobile.com****, Hui Xu** **xuhui@catt.cn**

*Abstract: A use case of flexible and secure network sharing scenarios is proposed and potential requirements are described for the shared network without direct connection between NR-RAN and 5GC in TR22.851.*

**1. Introduction**

Compared with 5G Multi-Operator Core Network (5G MOCN) network sharing, the shared network without direct connection between radio access network of Hosting operator and core network of Participating operators(a.k.a non-N2 sharing network) will provide a more flexible deployment to extend the network availability of home network operator regardless of N2 connection existence or not. Also, the interconnection between core networks will inevitably expose more user-specific information across the networks of Host and Participating operators, which requests further investigation on the user data privacy and security impact. The document aims to study use case of flexible and secure non-N2 shared network and potential requirements.

**2. Reason for Change**

Service availability and security aspects shall be addressed for shared network through interconnection between core networks and introduced to Section 5 “Use Cases” of TR 22.851.

**3. Conclusions**

<Conclusion part (optional)>

**4. Proposal**

It is proposed to agree on the following changes to 3GPP TR22.851 v0.1.0

\* \* \* First Change \* \* \* \*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

1. 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
2. 3GPP TS 22.101: "Service principles".
3. 3GPP TS 22.261: "Service requirements for the 5G system".

[x1] 3GPP TS 22.104: "Service requirements for cyber-physical control applications in vertical domains".

[x2] 3GPP TS 33.105: "Security architecture and procedures for 5G system".

\* \* \* Next Change \* \* \* \*

# 5 Use cases

## 5. X Use case of flexible and secure shared network

### 5.X.1 Description

The service availability is one important KPI for 5G system as stated in TS 22.261[3] and even critical in some vertical domains as TS22.104[x1] In live network, the connection between dedicated radio access network and home core network will not always be available due to unforeseen issue (e.g. fiber cut), which will break the service availability sometimes. Once happen, how to quickly recover the service is very important to ensure guaranteed user experience and reduce side effect and user complaint.

The network planning in a specific region has been done in advance during the rollout, thus it’s not easy to deploy a backup base station in a short time. Shared RAN of 5G MOCN network could be an option to solve the unavailability issue temporarily if the home core network has already deployed N2 connection between shared RAN and home core network. However, in the case there is no N2 connection deployment and provisioning ahead, new network sharing solutions (e.g. Interconnection between core networks) shall be well studied to provide alternative options to ensure the communication service availability.

5G core network based on service-based architecture natively supports more flexible deployment scenarios than before. Also, the current network architecture has already taken multiple PLMN interconnection scenarios into account (e.g. roaming) and been prepared in network elements and interfaces. Even if the network sharing through interconnection between core networks is not considered in the original rollout plan, it is possible to deploy and enable this feature immediately with lightweight change regarding the operator agreement on network sharing.

Along with the interconnection between different core networks, the user data privacy and security aspects shall be well considered.

### 5.X.2 Pre-conditions

Two network operators, OP1 and OP2, have deployed their respective radio access network in a country. The networks cover different parts of the country but overlap in a certain region.

There is an agreement between OP1 and OP2 to build a shared network with different strategies in different coverage areas as illustrated in Figure 5.X.2-1.

For UE1 and UE 2, who are the subscribers to OP2, the following assumptions are applied.

* OP1 is a service provider of PLMN, acting as Hosting Operator of a shared network.
* OP2 is a service provider of PLMN or SNPN, acting as Participating Operator of a shared network.
* OP1 NG-RAN has direct connection to OP2 5GC in Area A.
* OP1 NG-RAN has no direct connection to OP2 5GC but interconnection between their 5GCs in Area B.
* OP2 NR-RAN is deployed in Area C.
* OP1 and OP2 support the mobility between shared RAN to their respective RAN.



**Figure 5.X.2-1: Flexible and Secure Shared Network**

### 5.X.3 Service Flows

1. UE 1 and UE 2 power on in Area B, and register to OP2 through OP2 NG-RAN successfully.
2. Suddenly, the backhaul of OP2 NG-RAN to OP2 5GC is lost.
3. UE 1 and UE 2 reselect to OP1 NG-RAN and update service registration in OP2 through OP1 network, with the information of subscription and network element transferred between OP2 and OP1 under security protection.
4. UE 1 moves to Area A with or without active service.
5. UE 1 updates service registration in OP2 through OP1 NG-RAN with the information of subscription and network element transferred between OP2 and OP1 under security protection.
6. UE 2 moves to Area C with or without active service.
7. UE 2 update service registration in OP2 through OP2 network with the information of subscription and network element between OP1 and OP2 under security protection.

The information related to serving network elements may be transferred during an active communication, for example, IP address and network element identification.

The necessary information of border element between networks of Hosting operator and Participating Operator are known in order to serve the normal network connection. At the same time, the non-border element information of one operator’s network should be hidden from the other operator’s network to as large extent as possible.

### 5.X.4 Post-conditions

UE 1 and UE 2 keep single registration to OP2.

UE1 and UE 2 have no awareness of the update of service registration in OP2 through OP1 network, with the information of subscription and network element transferred between OP2 and OP1.

### 5.X.5 Existing features partly or fully covering use case functionality

Network sharing with interconnection between core networks is not excluded from the requirements of network sharing in 3GPP TS 22.101 [2]:

*Network sharing shall be transparent to the user.*

*The specifications shall support both the sharing of:*

*(i) radio access network only;*

*(ii) radio access network and core network entities connected to radio access network.*

The service and security requirements for 5G system across operators are mentioned in 3GPP TS 22.261[3] as below:

In service delivery across operators aspects,

*For a user with a single operator subscription, the use of multiple serving networks operated by different operators shall be under the control of the home operator.*

*In the event of the same service being offered by multiple operators, unless directed by the home operator's network, the UE shall be prioritized to receive subscribed services from the home operator's network.*

*NOTE 2: If the service is unavailable (e.g. due to lack of network coverage) from the home operator's network, the UE may be able to receive the service from another operator's network.*

In security aspects,

*The 5G system shall support a mechanism for the operator to authorize subscribers of other PLMNs to receive temporary service (e.g. mission critical services).*

*The 5G system shall enable an NPN to be able to request a PLMN to perform NPN access network authentication of a UE based on 3GPP identities and credentials supplied by the PLMN.*

Regarding TS 33.501[x2], the networks from different operators are assumed to lie in different trust zone. Message traverses trust boundaries shall follow the security requirements for service registration, discovery and authorization:

*NF Service based discovery and registration shall support confidentiality, integrity, and replay protection.*

*NRF shall be able to ensure that NF Discovery and registration requests are authorized.*

*NF Service based discovery and registration shall be able to hide the topology of the available / supported NF's in one administrative/trust domain from entities in different trust/administrative domains (e.g. between NFs in the visited and the home networks.)*

*NF Service Request and Response procedure shall support mutual authentication between NF Service Consumer and NF Service Producer.*

*Each NF shall validate all incoming messages. Messages that are not valid according to the protocol specification and network state shall be either rejected or discarded by the NF.*

The solution for E2E core network interconnection security shall satisfy:

*The solution shall provide confidentiality and/or integrity end-to-end between source and destination network for specific message elements identified in the present document. For this requirement to be fulfilled, the SEPP shall be present at the edge of the source and destination networks dedicated to handling e2e Core Network Interconnection Security. The confidentiality and/or integrity for the message elements is provided between two SEPPs of the source and destination PLMN–.*

*The destination network shall be able to determine the authenticity of the source network that sent the specific message elements protected according to the preceding bullet. For this requirement to be fulfilled, it shall suffice that a SEPP in the destination network that is dedicated to handling e2e Core Network Interconnection Security can determine the authenticity of the source network.*

*The solution should have minimal impact and additions to 3GPP-defined network elements.*

### 5.X.6 Potential New Requirements needed to support the use case

[PR 5.X.6-001] The 5G system shall support a mechanism to enable Participating Operators to authorize the shared network on the interface operation and information exchange when UEs cross the border of shared networks and respective operator's network.

 [PR 5.X.6-002] The 5G system shall support a mechanism to authorize the subscribers of Participating Operators in the shared network to obtain the service with the minimum information exposure of the subscription and identities.

[PR 5.X.6-003] The 5G system shall minimize the information exposure related to non-border network elements, e.g. geographical location, network topology, etc. between the Hosting Operator’s and Participating Operators.

 [PR 5.X.6-004] The 5G system shall support a mechanism to transfer the user data with confidentiality and integrity protection between the networks of Hosting Operator’s and Participating Operators.

[PR 5.X.6-005] Based on mutual agreement, the 5G system shall support optimal network selection between home operator’s network and shared network regarding the network state (e.g., during congestion, disaster, emergency and DDoS events)

[PR 5.X.6-006] Based on mutual agreement, the 5G system shall support the Hosting operator to select the network sharing method in a given coverage area.

[PR 5.X.6-007] The shared network shall have minimal impact and additions to the existing 5G network architecture and elements.

\* \* \* End of Changes \* \* \* \*