**3GPP TSG-SA3 Meeting #99e *S3-201239-r1***

**e-meeting, 11 – 15 May 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.819** | **CR** | **0004** | **rev** | **2** | **Current version:** | **16.0.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps | **x** | ME | **x** | Radio Access Network | **x** | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | KI on service continuity - threats and reqs |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell , Interdigital |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | FS\_VERTICAL\_LAN\_SEC |  | ***Date:*** | 15.5.2020 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** | Rel-16 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)Rel-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | Resolution of FFSs is needed. Threats and requirements are FFS, but It is concluded that no normative work for this key issue is required, since it is addressed by the existing specification. |
|  |  |
| ***Summary of change:*** | Resolution of the 2 FFSs. |
|  |  |
| ***Consequences if not approved:*** | Unresolved FFSs |
|  |  |
| ***Clauses affected:*** | 5.2.2.2, 5.2.2.3 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **x** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** | S3-200378 |

\*\*\*\*\*\*\*\* START OF CHANGES

### 5.2.2 Key Issue #2.2: Security and privacy aspects of service continuity and session continuity

#### 5.2.2.1 Key issue details

**Background**

Clause 3.1 of the present document contains definition of service continuity and session continuity, as specified in 3GPP TS 23.501 [7].

Service continuity and session continuity do not mean transfer of service and session from PLMN to NPN and vice-versa. The continuity is in the sense of transfer from native connective to tunnelled connection, and vice-versa. In other words, there is no "roaming" (in the same sense that we use across PLMNs) between PLMN and NPN.

3GPP TS 23.734 uses the term service continuity in its key issues and solutions. That is fine because support for service continuity would cater session continuity as well. Regarding the key issue #6, i.e., access to PLMN services via NPN and vice-versa, 3GPP TS 23.734 [3] has concluded that solution #20 is chosen as baseline for normative work. Further, it has also concluded (according to solution #21) that seamless service continuity between PLMN and NPN is achieved by dual radio support and there no protocol changes.

In short, the chosen solution #20 works in the following way - one network (PLMN or NPN) treats another network (NPN or PLMN) as a non-3GPP access and tunnels communication using another network's N3IWF. See Figure 5.2.2.1-1.

|  |  |
| --- | --- |
|  |  |
| Figure 5.2.2.1-1: Baseline architecture for accessing PLMN via NPN (left) and NPN via PLMN (right) |

**Description**

This key issue is about investigating security aspects of service and session continuity when accessing PLMN services via NPN and vice-versa. In other words, this key issue is for analysing IF and WHAT "new" security mechanisms would be required for the solution #20 in 3GPP TS 23.734 [3].

There are several aspects that are worth investigating for security and privacy impacts, e.g., because of:

- Nwu interfaces (NwuPLMN and NwuNPN) between UEs and PLMN/NPN N3IWFs;

- both the PLMN and the NPN having own security contexts for UEs even though a single radio is used;

- UEs discovering one network's N3IWF via another network's radio;

- UEs performing PDU Session(s) handover from NPN N3IWF to NPN 3GPP RAN, and PLMN 3GPP RAN to PLMN N3IWF;

- UEs performing PDU Session(s) handover from PLMN N3IWF to PLMN 3GPP RAN, and NPN 3GPP RAN to NPN N3IWF;

- etc.

#### 5.2.2.2 Security threats

It is concluded that no normative work for this key issue is required, since it is addressed by the existing specification. Thus, security threats for this key issue are not addressed in the present document.

#### 5.2.2.3 Potential security requirements

It is concluded that no normative work for this key issue is required, since it is addressed by the existing specification. Thus, potential security requirements for this key issue are not addressed in the present document.

\*\*\*\*\*\*\*\* END OF CHANGES