**3GPP TSG-SA3 Meeting #113 *S3xxxx***

**Chicago, US, 6 - 10 November 2023** **(revision of S3ah-230021, S3-233898-r3)**

**Source: Nokia, Nokia Shanghai Bell, U.S. National Security Agency, NIST, CableLabs, China Telecommunications**

**Title: New SID on resource isolation enforcement for application in 5G network**

**Document for: Approval**

**Agenda Item: 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](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: Study on resource isolation enforcement for application in 5G network

{Free text. It has to be the same as in the "Title:" section above. Studies have to start by "Study on"}

Acronym: FS\_APPRES\_ISO

Unique identifier: TBA

Potential target Release: Rel-19

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  | X | X | X |  |
| No |  |  |  |  |  |
| Don't know | X |  |  |  | X |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
| X | Study  |
|  | Normative – Stage 1 |
|  | Normative – Stage 2 |
|  | Normative – Stage 3 |
|  | Normative – Other\* |

**\* Other = e.g. testing**

## 2.2 Parent Work Item

For a brand-new topic, use “N/A” in the table below. Otherwise indicate the parent Work Item.

|  |
| --- |
| Parent Work / Study Items: N/A |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
|  |  |  |  |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
|  |  | {optional free text}  |

# 3 Justification

5G is now deployed in many countries/regions, and operators keen to monetize the network with offering diverse services to different vertical customers. 5G will be able to support extreme and diverse requirements for throughput, latency, availability and capacity. Security is another fundamental network requirement that needs to be optimized for each specific use case, especially for those uses cases where security becomes critical (e.g., V2X platooning, enterprise VPN or Electric grids). Operator allocates 5G network resources to vertical/enterprise customers to support various use cases and applications, the resource can be isolated from networks or network resources used by other cellular customers. Network slicing is a key feature and business driver for 5G, which enables enterprises and operators to address specific requirements of different market segments (e.g., industrial, smart cities, healthcare, automotive). The overall security architecture of 5G network is enhanced with new security features, available as well in network slices as logical networks created within the 5G network.

A business wants to have a secure and isolated set of network capabilities that meets its communication needs, without having to purchase and maintain the network infrastructure. Isolation is a multi-faceted problem, on security dimension, it’s ensuring that any type of intentional attack occurring in one collection of network functions /resources have no impact on any other network functions/resources. With the corresponding slice specific enforcements, slice security isolation can prevent unauthorized access and modification to data, processes, services or functions.

Both operators and their vertical customers expect the application traffics can be isolated and protected properly from UE, to access network, to 5G core network, to data network based on security SLA, operator security policies, regulations, etc. In addition, the operators and verticals expect the network resources, including infrastructure resources, allocated to support the applications can be isolated properly as well.

Some Isolation requirements on network slice were raised in GSMA (e.g. GSMA NG.135, GSMA NG.127) and also defined in 3GPP TS (e.g. 3GPP TS 22.261) or discussed in 3GP TRs (e.g. 3GPP TR 33.848, TR 33.864). Please see the discussion paper S3-23xxxx for the detail.

3GPP developed specifications to support network slice deployment and configuration. E.g. management services (including network resource model) and procedures defined in 3GPP SA5 (3GPP TS 28.541, TS 28.533, TS 28.531) enables mapping slice SLA to attributes of network slice and network slice subnet, then further translating those attributes to slice related configuration parameters of NR and 5GC NFs. The MnSs and procedures also support to deploy and scale the NFs, either in physical device or cloudified infrastructure, to satisfy the slice requirements. Please see the discussion paper S3-23xxxx for the detail

However, there’re still some gaps in current specification to fulfil security requirements of application, and enforce application isolation in 5G network:

1. Lack of isolation at network resource layer as lack of supporting interface which may cause unnecessary communication between NFs supporting different network slices for the applications. Further, a compromised or malicious low security profiled network slice may impact a highly sensitive slice, e.g. steal services/resources and data of mission critical applications.
2. Virtualization infrastructure is not properly isolated and protected for different applications as lack of coordination between 5G system and cloud system, that may incur sensitive data of one application exposed to VNFs/CNFs of other applications through side channel attacks, compromised hardware or software component, etc., although the access control is correctly performed on SBI based 5GC network.

For example, operator may deploy several slices to support different business cases of vertical customers, who makes plan to assign different business applications to corresponding slices, and isolate the slices based on security requirements from the customers, security policies of operators, regulations, and other non-security related criteria, etc. As isolation related information model is not supported in existing specifications, the isolation plan cannot be mapped to attributes of network slice, network slice subnet, network function, or infrastructure requirements. Therefore, the domain management functions (e.g. RAN/CN network slice subnet management functions (NSSMFs) and RAN/CN network function management functions (NFMFs) from different vendors) cannot translate the isolation requirement to corresponding network and network function configuration. Finally, the resource may not be correctly selected and allocated, e.g. resource may be still shared between slices expected to be isolated with each other, and the NFs of different slices may be able to communicate with each other even they’re expected to be separated.

Those issues may be exploited by threat agent to launch attack towards mission critical slice through other poor secured /vulnerable slices, that may hinder the operators to offer the 5G network or network slice as service to vertical customer as lack of confidence on resource isolation and protection, then limit the commercial use case for operators.

# 4 Objective

Study how to enable verticals, operators and cloud service providers to address diverse requirements of different market segments for security and isolation, and to holistically investigate the gaps in existing specification and collect potential solutions to enforce resource isolation for applications in 5G network.

1. Clarify resource isolation concept especially in security point of view.
2. Investigate the gaps of existing specification on network and virtualization resource isolation and protection for vertical applications.
3. Collect potential solutions to fulfil differentiated security SLA of enterprise applications and enforce resource isolation and correct resource selection for applications in 5G network, hence satisfy the security requirements of various business cases from different industries and improve compliance with industry regulatory and business requirements.

## TU estimates and dependencies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Work Task ID | TU Estimate(Study) | TU Estimate(Normative) | RAN Dependency(Yes/No/Maybe)  | Inter Work Tasks Dependency Editor’s Note: This column should highlight if WT#x is self-contained, or is dependent on completion of other WTs |
| 1. | 1.5 TUs (3 meeting cycles) | 1 TUs (2 meeting cycles) | No | The SI is not dependant on other WTs but may raise requirements on SA5 to enhance network information model for security isolation. |
| 2. |  |  |  |  |
| 3. |  |  |  |  |

Total TU estimates for the study phase: 1.5 TUs (3 meeting cycles)

Total TU estimates for the normative phase: 1 TUs (2 meeting cycles)

Total TU estimates: 2.5

# 5 Expected Output and Time scale

***{If this WID covers both stage 2 and stage 3, clearly indicate the different completion dates.}***

|  |
| --- |
| New specifications {One line per specification. Create/delete lines as needed} |
| Type  | TS/TR number | Title | For info at TSG#  | For approval at TSG# | Rapporteur |
| Internal TR | 33.xyz | Study on resource isolation enforcement for application in 5G network  | SA#102(Dec-23) | SA#104(June-24) | Jing Ping, Nokia, jing.ping@nokia-sbell.com |
|  |  |  |  |  |  |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| N/A | N/A | N/A | N/A |
|  |  |  |  |

# 6 Work item Rapporteur(s)

Jing Ping, Nokia, jing.ping@nokia-sbell.com

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

Stage 3 aspects covered by CT WGs, probably SA5

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Nokia |
| Nokia Shanghai Bell |
| U.S. National Security Agency |
| NIST |
| CableLabs |
| China Telecommunications |
| KDDI |
| ZTE |
| Vodafone |
| Verizon |
| MITRE |
| Johns Hopkins |
| Xiaomi |
| T-Mobile |
| Deutsche Telekom AG |
| InterDigital, Inc. |
| Telefónica |