**3GPP TSG-SA3 Meeting #115 *S3-240613r1***

**Athens, GR, 26 February to 01 March 2024**

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

**Title: New SID on enhancement of 5G network slice security**

**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 enhancement of 5G network slice security

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

Acronym: FS\_NSRES\_ISO

Unique identifier: TBA

Potential target Release: Rel-19

# 1 Impacts

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

## 3.1 network slice resource isolation

5G is now deployed in many countries/regions, and operators keen to monetize the network with offering diverse services to different vertical customers and supporting 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., vehicle platooning, enterprise VPN, public safety or Electric grids). 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. E.g. with the corresponding slice specific enforcements, slice security isolation can prevent unauthorized access and modification to data, processes, services or functions. Examples of expected network slice isolation in deployment are described as follows:

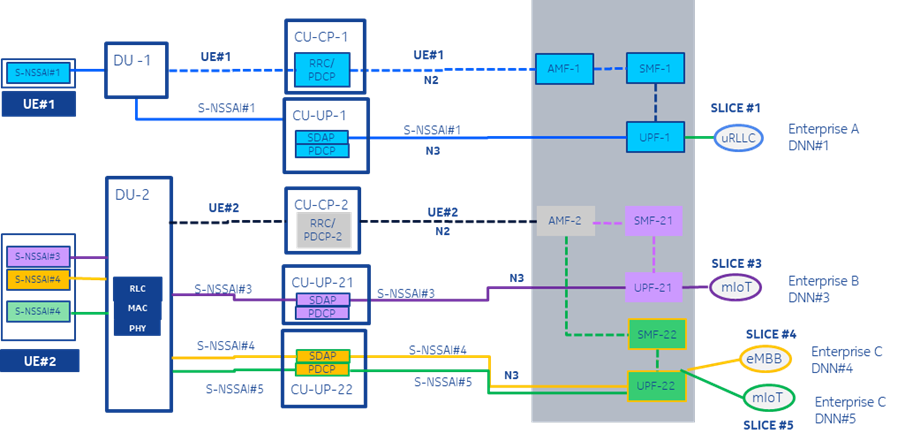


Figure 1 network slice isolation use cases

A slice is fully isolated from other slices, from RAN to transport to CN, and from control plane (CP) to user plane (UP), dedicated resources are allocated to the slice, e.g. S-NSSAI#1

A slice is partially isolated from other slices, e.g. share DU and other CP NFs, but use dedicated UP related NFs, e.g. S-NSSAI#3

A slice shares all NFs with other slices, e.g. share DU, CU, CP and UP NFs, e.g. S-NSSAI#4 and 5

A screenshot of a computer

Description automatically generated

Figure 2: Expected resource allocation with proper isolation

As shown in the above Figure 1, operator expects the resources allocated for a network slice are separated in multiple layers, e.g. logical network layer (such as Network Slice and Network Slice Subnet defined in SA2 or SA5), network resource layer (such as Managed Function defined in SA5 or Network Function defined in SA2) and infrastructure layer (out of 3GPP scope). However, there’re still some gaps in current specification to fulfil security requirements of slice and enforce slice isolation in 5G network. Lack of isolation and protection at network resource layer represented as a set of network functions and the associated resources (e.g. network slice subnet defined in TS 28.530 or Network Slice instance defined in TS 23.501) may cause unnecessary communication between NFs supporting different network slices. Those issues may be exploited by threat agent to launch attack towards mission critical slice through other poor secured /vulnerable slices, e.g. steal services/resources and data of mission critical applications. GSMA was reported a number of findings about 5G Slicing Vulnerabilities, e.g. CVD-2021-0047, CVD-2023-0069, which are related to slicing security isolation in some extent.

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, TS 28.531, TS 28.541). But it's either too abstract to be implementable (e.g. requirements in TS 22.261) or missed security aspects (e.g. requirements, use case and information model in TS 28.531, 28.541). There is no clear definition and requirement on slicing security isolation in 3GPP so far.

## 3.2 end-to-end slice data protection

Current TS 33.501 covers network slice specific access authentication and authorization that could address User ID and credentials different from 3GPP subscription credentials. But, TS 33.501 does not address the end-to-end protection of the user data transmitted within the slices.

Solutions relying on over-the-top applications to protect user data in integrity or confidentiality or both require expertise from the users to install the solutions. Consequently, the user data transmitted within slices may not be properly protected. Additionally, the attack surface increases, and there is also the risk that the devices may not support solutions relying on over-the-top applications.

To guaranty seamless security and privacy of user data exchanged within slices, an end-to-end protection for slice data should be defined by 3GPP.

# 4 Objective

Study enhancement on network slicing security to support network slice security isolation and end to end slice data protection .

WT1: Study diverse requirements of different market segments with considering security and isolation, and to investigate the gaps in existing specification and collect potential requirements to enforce slicing security isolation in 5G network.

* Document the concept and definition of slicing security isolation, based on slice isolation requirements defined in GSMA and TS 22.261, and slice management and isolation use case and information model defined in 3GPP TS 28.530, 28.541 and 23.501.
* Further investigate/study slicing isolation requirements in SA1 and SA5, and define finer grained slicing isolation security requirements.
  + Note: The slicing isolation security requirements may be provided to SA5 to update their slicing management services and procedures.

WT2: Study end-to-end protection of user data transmitted within slices. The end-points of this end-to-end protection are the UE and 3rd party or operator who owns an AAA server (AAA-S) used to perform network slice specific authentication and authorization procedure. This study takes into account the Lawful Interception aspects, and architecture defined by SA2

## 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. | 1.0 TUs | 1 TUs | No | The SI is not dependant on other WTs but may raise requirements on SA5 to enhance network information model for security isolation. |
| 2 | 1.5 TUs | 0.5 TUs | No |  |

Total TU estimates for the study phase: 2.5 TUs (4 meeting cycles)

Total TU estimates for the normative phase: 1.5 TUs (2 meeting cycles)

Total TU estimates: 4

# 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) | TBD |
|  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 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)

TBD

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

The slicing isolation security requirements may be provided to SA5 to update their slicing management services and procedures.

# 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 |
| Google |
| OTD US |
| BT |
| NCSC |
| NTIA |
| Lenovo |
| Thales |