**3GPP TSG-SA3 Meeting #105-e *S3-220426r5***

e-meeting, 14 - 25 February 2022 (revision of S3-yyxxxx)

**Source: Lenovo, Motorola Mobility, Interdigital, Verizon, Cablelabs, Mavenir, Johns Hopkins University APL, LG Electronics, Telefonica, NEC, Telia Company, AT&T, Samsung, Broadcom, PCCW Global B.V, China Mobile, Motorola Solutions, Inc, Nokia, Nokia Shanghai Bell, Intel**

**Title: Study on Zero Trust Security**

**Document for: Approval**

**Agenda Item: 4.18**

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 Zero Trust Security

Acronym: FS\_ZTS

Unique identifier: TBD

{A number to be provided by MCC at the plenary}

Potential target Release: Rel-18

# 1 Impacts

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

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
|  | Feature |
|  | Building Block |
|  | *Work Task* |
| x | Study Item |

## 2.2 Parent Work Item

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

### 2.3 Other related Work Items and dependencies

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

**Dependency on non-3GPP (draft) specification:** N/A

# 3 Justification

Zero Trust enables a transition from network defense towards a more proactive in-advance security to be in place to combat the security threats if occur due to any malicious operations or compromised network functionalities. The core principle of Zero Trust [1] includes continuous trust validation (i.e., monitoring the state) and minimizing impacts if any security breach occurs due to external factors (example., botnets) or by an insider.

The existing 5G system security is built on certain key principles that include authentication, authorization, and secure connection establishment, but the current system does not provide a continuous or as needed dynamic mechanism to evaluate the trust of the involved communication endpoints. But due to the heterogeneity and varied NF deployment options, the NF(s) may run into configuration issues, get exposed to insider threats, or face cyberattacks. So, the trust over NF or AF cannot be assumed static and intact throughout its lifetime.

Moreover, if any NF gets compromised in its lifetime, it may impact UEs services and may impact other connected NFs (i.e., through the lateral movement of attack). Therefore adaptation of Zero Trust approach in addition to the current security mechanisms can provide the tools to allow dynamic on demand trust evaluation, advanced threat detection, detection of threat lateral movement which may causefurther compromises; thereby limiting the threat’s impact and reach while ensuring the service continuity.

The adaption of ‘Zero Trust’ approach for 5GS security can facilitate the realization of potential benefits for vertical service customers and business and also ensure service reliability and safety. Therefore, it is proposed to analyse the existing 5G system to see if it can be benefitted with the principles of Zero Trust security. When required the study will recommend the potential way(s) to evaluate and ensure trust in the 5G system.

[1] NIST Special Publication 800-207, ‘Zero Trust Architecture’, August 2020.

# 4 Objective

Analyse the 3GPP 5GS security scenarios that may benefit from a Zero Trust approach and identify the associated threats.

Analyse the suitable Zero Trust security approach to address the threats identified where potential security risk exists.

Provide recommendations for a Zero Trust 5GS security, where such recommendations may include 3GPP 5G security requirements, technical enhancements, and procedural enhancements.

The scope of the study is limited to adapt zero trust in the core network for the current release.

# 5 Expected Output and Time scale

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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.xxx | Study on Zero Trust Security | TSG#98 | TSG#99 | Sheeba Backia Mary B, Lenovo, Motorola Mobility, smary@lenovo.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)

Sheeba Backia Mary B, Lenovo, Motorola Mobility, smary@lenovo.com

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Lenovo |
| Motorola Mobility |
| Interdigital |
| Verizon |
| Cablelabs |
| Mavenir |
| Johns Hopkins University APL |
| LG Electronics |
| Telefonica |
| NEC |
| Telia Company |
| AT&T |
| Samsung |
| Broadcom |
| PCCW Global B.V |
| China Mobile |
| Motorola Solutions, Inc |
| Nokia |
| Nokia Shanghai Bell |
| Intel |
|  |
|  |
|  |
|  |
|  |