**3GPP TSG-SA3 Meeting #107-eS3-221004**

e-meeting, 16 - 20 May 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, PCCW Global B.V, China Mobile, Motorola Solutions, Inc, Nokia, Nokia Shanghai Bell, Intel, NTT DOCOMO INC., Ericsson, Rakuten Mobile Inc, China Telecom, Charter Communications, Center for Internet Security, Public Safety Canada, US NSA**

**Title: Study on Zero Trust 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 applicability of Zero Trust Security principles in mobile network

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 |  |
| No |  |  |  |  |  |
| Don't know | x | 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 principle enables a transition from static network defense towards a more proactive security paradigm to combat security threats from any malicious operations or compromised network functionalities. A core principle of Zero Trust [1] includes continuous trust validation (i.e., monitoring the state, access control policies, and real-time verification) and minimizing impacts if any security breach occurs due to external factors or by an insider. A Zero Trust strategy enables more rapid detection, isolation, and response to different threats [2]. Therefore, these factors highlight the importance of Zero Trust principles to enable advanced security measures that drastically reduce the risk of successful cyber-attacks against infrastructure and services.

Due to the heterogeneity and varied NF deployment options, the NF(s) may experience configuration issues, encounter insider threats, or face cyberattacks. So, the trust over NF or AF cannot be assumed static and intact throughout its lifetime. The existing 5G system security supports certain aspects of Zero Trust principle such as authentication, authorization, and secure connection establishment, but the current system does not support a continuous or on-demand dynamic mechanism to evaluate the trustworthiness of the involved communication endpoints which is a key tenet of Zero Trust principle. The current system also does not support a mechanism to use any insight from evaluations of trust to improve its security posture (e.g., dynamic policy creation and enforcement).

Moreover, at any time during its life cycle a compromised NF may impact UEs services as well as other connected NFs (i.e., through the lateral movement of an attack). Therefore, adopting the Zero Trust principle in addition to the current security mechanisms can provide the tools to allow dynamic on demand trust evaluation, access to resources determined by dynamic policy, advanced threat detection, and detection of lateral movement. Thereby prevent further compromises; and limiting the threat’s impact while ensuring service continuity.

The adaption of a ‘Zero Trust’ principle for 5GS security can facilitate the realization of potential benefits for vertical service customers and business and also can ensure service reliability and safety. Therefore, it is proposed to analyse the existing 5G system to identify additional opportunities to apply principles of Zero Trust security. Where required the study will identify potential areas that can benefit from Zero Trust principles, solicit solutions, evaluate the benefits of increasing the trust and as applicable recommend the potential way(s) to evaluate and ensure trust in the 5G system. Where applicable, the study can also take into account the progress in the other SA3 works e.g., eSBA, eNA, etc., The scope of the study will focus on aspects to adapt zero trust principle in the core network.

NOTE: The study will not consider any application of Zero Trust security principle or trust evaluation process for access network and UE.

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

[2] US Executive order related to Zero Trust Architecture, ‘https://www.whitehouse.gov/omb/briefing-room/2022/01/26/office-of-management-and-budget-releases-federal-strategy-to-move-the-u-s-government-towards-a-zero-trust-architecture/’, January 2022.

# 4 Objective

The objective of the study includes:

1. Analyse the 3GPP 5GS security scenarios related to the 5G core network that may benefit from a Zero Trust principle and identify the associated threats.
2. Analyse the suitable Zero Trust security mechanisms (i.e., for enabling trust evaluation and ensuring trust) to address the threats identified where potential security risk exists.
3. Provide recommendations for support of additional Zero Trust principles in 5GS security architecture, where such recommendations may include 3GPP 5G security requirements, technical enhancements, and procedural enhancements.

# 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, 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 |
| PCCW Global B.V |
| China Mobile |
| Motorola Solutions, Inc |
| Nokia |
| Nokia Shanghai Bell |
| Intel |
| NTT DOCOMO INC. |
| Ericsson |
| Rakuten Mobile Inc |
| China Telecom |
| Charter Communications |
| Center for Internet Security |
| Public Safety Canada |
| US NSA |