**3GPPSA3-e(AH) for Rel-19 SID/WID workshop *S3ah-230012***

**Online 26-27 September 2023** **(revision of xx-yyxxxx)**

**Source: Lenovo, Motorola Mobility, MITRE, Interdigital, Motorola Solutions, Charter Communications, Johns Hopkins University APL, Intel, US National Security Agency, Telefonica, NCSC, OTD\_US, Deutsche Telekom, Keysight Technologies, Center for Internet Security, SDI Squared, Cablelabs, IIT Delhi, Philips International B.V., Nokia, Nokia Shanghai Bell, Samsung, NEC, Rakuten Mobile, Peraton Labs, CISA ECD, NTIA, Department of Telecom, British Telecom, NDRE, T-Mobile, AT&T**

**Title: New SID on enablers for Zero Trust Security**

**Document for: Approval**

**Agenda Item: 3**

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 enablers for Zero Trust Security

Acronym: FS\_eZTS

Unique identifier:

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

Potential target Release: Rel-19

# 1 Impacts

{For Normative work, identify the anticipated impacts. For a Study, identify the scope of the study}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  |  |  | x |  |
| No | x | 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

|  |
| --- |
| Parent Study Items  |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| FS\_ZTS | SA3 | 960038 | Study on applicability of the Zero Trust Security principles in mobile networks |

### 2.3 Other related Work Items and dependencies

{List here other Work Items which relate to the proposed one, such as a Work Item in an earlier Release if further enhancing the feature from the previous Release)}

|  |
| --- |
| 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

The 5G system was designed with core security features to support authentication, communication security and authorization which form the basis of Zero Trust security [1]. Nevertheless, the ZT core principle also insists to ‘assume breach and verify explicitly’ to improve the security posture and if an attack happens to prevent lateral threat movement. An effective Zero Trust deployment is dependent on an effective set of security controls to assess, detect and report attacks on the 5G system. In the ZT concept, these can be viewed as the inputs for zero trust security policy(ies). Under the assumption of a breached 5G network when there is no sufficient mechanism(s) to detect the attacks and related abnormalities, further lateral movement will be unhindered. Furthermore, it may be possible for the malicious actor to gain unauthorized access and exfiltrate/manipulate network/service(s) data.

The 5G system supports mechanisms as described in TS 23.288 clause 6.7.5 [2] to identify abnormal UE behaviour, i.e., mechanisms described in [2] identifies risks (e.g., DDoS suspicion), and report abnormal behaviour statistics and predictions. With the reported abnormal behaviour information, access control for UE(s) is improved with NF(s) actions (e.g., PCF requests SMF to release the PDU session; SMF releases the PDU session and apply SM back-off timer). On the other hand, there exists no 5G system security mechanisms to identify NF(s) abnormal behaviours and risks in the 5GC.

Due to the heterogeneity and varied NF(s) deployment options, there is a chance that a NF(s) may experience configuration issues, modification in access privilege levels, encounter insider threats, or face cyberattacks. Thus, static trust of a NF and its behaviour should not be assumed to be intact and normal throughout its lifetime. If a NF behaves abnormally, there should be a means to identify and improve the security controls as applicable in real-time. Real-time identification and security control changes have not yet been standardized in 3GPP (presuming each Network operator deployed their own choice of SIEM system).

There were Rel.18 initiatives [1] undertaken to study the Zero Trust security principles. [1] provides a detailed security evaluation for Zero Trust Tenets 1,2,3, 4, 5, 6, and 7, and suggests required data collection to enable continuous security monitoring and evaluation. Further in Tenet 5 evaluation, it clarifies the need to define and specify the information that is exposed by the NF(s) for security monitoring. Also, Tenet 6 evaluation, states that, ‘at the 3GPP SBA layer one can investigate whether there is any additional information that could be exposed for security monitoring purposes and how such information is used for access control decisions e.g., authorization. There is an ongoing global effort to adapt Zero Trust security principles [5][6][7][8][9][10][11][12] to overcome the emerging attack surface and lateral threat movement within the network. Meanwhile SA5 has also endorsed ‘Enablers for Security Monitoring’ as the Rel.19 study topic and cited SA3 as the collaboration group for this topic [3]. Therefore, it is proposed to consider the recommendations from Tenet 4,5,6, and 7 evaluation information [1], analyse the following, and identify necessary security adaptions as required [4]:

* For any NF that is compromised or exhibits abnormal behaviour, 3GPP security controls and mechanisms are needed to:
	+ Identify the NF that has been compromised/behaving abnormally.
	+ Prevent lateral attack movement and ensure continuous service availability (simply terminating/isolating a compromised or misbehaving NF(s) would impact all the ongoing services).
	+ Collect and report abnormal behavior related data (for external security analysis/monitoring) and to enable OAM security functions to use the results and in response provide appropriate actions to prevent threat of lateral movement and ensure service availability.
	+ Automatically identify and correct compromise means to ensure the replacement NF will not be compromised in the same manner.

References:

[1] 3GPP TR 33.894, ‘Study on applicability of the Zero Trust Security principles in mobile networks’, Release 18.

[2] 3GPP TS 23.288, ‘Architecture enhancements for 5G System (5GS) to support network data analytics services’, Release 18.

[3] S5-234823, ‘Enablers for Security Monitoring’, SA5 Collection of Rel-19 potential topics for SA workshop presentation, Endorsed.

[4] S3-23aaa, ‘Discussion Paper on Rel-19 Study on Network based Zero Trust Security’.

[5] NIST Special Publication 800-207, ‘Zero Trust Architecture’, [Zero Trust Architecture (nist.gov)](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf).

[6] National Security Agency, ‘Embracing a Zero Trust Security Model’, [CSI\_EMBRACING\_ZT\_SECURITY\_MODEL\_UOO115131-21.PDF (defense.gov)](https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF).

[7] ITU SG 17, ‘Guidelines for zero trust based access control platform in telecommunication network’, <https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=18032>.

[8] ITU SG 13, ‘Assessing trust evaluation models for telecommunication networks’, <https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18421>.

[9] Department of Defense (DOD), ‘Zero Trust Reference Architecture’, [Department of Defense Zero Trust Reference Architecture](https://dodcio.defense.gov/Portals/0/Documents/Library/%28U%29ZT_RA_v2.0%28U%29_Sep22.pdf).

[10] National Cyber Security Centre (NCSC), ‘Zero Trust architecture design’, <https://www.ncsc.gov.uk/collection/zero-trust-architecture/introduction-to-zero-trust>.

[11] ATIS, ‘Enhanced Zero Trust and 5G’, <https://www.atis.org/tops-council/enhanced-zero-trust-and-5g/>

[12] MITRE, ‘Achieving Mission Assurance for Enterprises today and tomorrow – Zero Trust, The cloud, and other Tools’, <https://apps.dtic.mil/sti/trecms/pdf/AD1172262.pdf>.

# 4 Objective

The Objective of the study includes:

Work Task (WT)

WT1 – Data exposure for security evaluation and monitoring

* WT1.1: Based on TR 33.894 KI#1 security requirement, conclusion, and Tenet 5 evaluation, for events which can lead to security threats, define the data to be exposed by the NF and define how those data can be securely exposed to the Operator’s security functions (e.g., SIEM) to enable the external security evaluation and monitoring.

NOTE: The external security evaluation and monitoring is up to operator’s implementation and outside the 3GPP domain. The aspects to enable OAM based data collection is up to SA5 WG. The necessary adaptations specific to exposure services for providing data to the external security function needs SA2 collaboration.

WT2 – Security mechanism to prevent lateral movement of threat

* WT2.1: Analyse the impacts and threats related to compromised NF(s) and abnormal NF behaviors.
* WT2.2: For NFs that have been identified as compromised or misbehaving, study how such information can be utilized to improve access control decisions at the NRF for employing appropriate security mitigations to prevent lateral movement and minimize impact to service availability.
* WT2.3: Study how 3GPP security policies and controls can be enhanced related to WT2.2 to mitigate threat lateral movement and service availability issues.

WT3 – Security enhancement recommendations

* Based on the study outcome, provide recommendations for network based security adaptation, where the recommendations may include but are not limited to requirements, technical enhancements, and procedural fixes.

## TU estimates and dependencies

|  |  |  |  |
| --- | --- | --- | --- |
| TU Estimate(Study) | TU Estimate(Normative) | RAN Dependency(Yes/No/Maybe)  | SA2 / SA5 Dependency(Yes/No/Maybe) |
| *WT1: 1* | *WT1,3: .5* | *No* | *May be* |
| *WT2: 1* | *WT2,3: .5* |
| *WT3: .5* | *-* |
| *Total: 2.5 TUs* *(5 meetings)* | *Total: 1 TUs* *(3 meetings)* |
| *NOTE: 1 TU is considered as 1.5 hours* |

Total TU estimates for the study phase: 2.5 TUs (5 meeting cycles)

Total TU estimates for the normative phase: 1 TUs (3 meeting cycles)

Buffer TU: .5 TU

**Total TU estimates: .4 TUs**

# 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 enablers for Zero Trust Security | TSG#102 | TSG#106 |  |
|  |  |  |  |  |  |

|  |
| --- |
| 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)

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

SA5 for the management services, SA2 for exposure services (as applicable)

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Lenovo |
| Motorola Mobility |
| MITRE |
| Interdigital |
| Motorola Solutions |
| Charter Communications |
| Johns Hopkins University APL |
| Intel |
| US National Security Agency |
| Telefonica |
| NCSC |
| OTD\_US |
| Deutsche Telekom |
| Keysight Technologies |
| Center for Internet Security |
| SDI Squared |
| Cablelabs  |
| IIT Delhi |
| Philips International B.V. |
| Nokia |
| Nokia Shanghai Bell |
| Samsung |
| NEC |
| Rakuten Mobile |
| Peraton Labs |
| CISA ECD |
| NTIA |
| Department of Telecom |
| British Telecom |
| NDRE |
| T-Mobile |
| AT&T |