**3GPP TSG-SA3 6G Workshop S3-xxx**

**Conference Calls, 6 - 7 August 2025** **(revision of xx-yyxxxx)**

**Source: Deutsche Telekom**

**Title: NF Authentication on Application Layer in 6G**

**Document for: Approval**

**Agenda Item:**

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: NF Authentication on Application Layer in 6G

Acronym: TBD

{Propose an acronym. Final acronym to be confirmed at the plenary. The sign "-" is a level separator between (Feature)-(Building Block)-(Work Task). The sign "\_" can be freely used. Studies have to start by "FS\_". Each acronym level has to be simple and short, 7 characters max recommended}

Unique identifier:

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

Potential target Release: Rel-20

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  |  |  | 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

|  |
| --- |
| 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 |
| N/A |  | {optional free text}  |

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

N/A

# 3 Justification

The integration of 5G networks into cloud infrastructure has introduced novel attack vectors and amplified existing security risks. This elevated risk profile stems not only from the disaggregation of hardware and software but also from the extensive array of potential NF implementation options as defined within 3GPP standards.

This broad interpretability significantly impacts the consistent and secure deployment of security standards across various implementations.

Therefore, the following question shall be discussed: Can the definition of the 3GPP standard be adapted in such a way that the implementation diversity is maintained but at the same time the security objective, in this case e2e NF authentication on application level, can also be achieved?

**The challenge**

The defined mechanisms in today's 5G standard assume one common endpoint for mTLS termination on transport level and authentication on NF application level.

Reality shows that NF implementations in cloud deployments do often not have this common implementation endpoint. They have an endpoint/instance handling mTLS termination (LB, gateway, pod, ...) and another instance/endpoint representing the NF/service. Currently, the endpoint handling mTLS termination is also the one being authenticated (on transport level). In other words, the intended authentication of the service/application which should be done on application level is done on transport level (mTLS).

This leads to

1. the situation that the point of authentication (mTLS termination endpoint – on transport level) and the point of authorization (NF/service on application level) are different (different PODs, different hosts, different physical instances,…)
2. the inability to deploy Layer 7 (L7) service meshes without relocating the authentication enforcement point away from the NF, as the application layer needs to be decrypted (mTLS termination) to be able to route to the called service path (in the HTTP header). Decryption at a point external to the NF introduces a potential security vulnerability by exposing unencrypted application data outside the trusted NF boundary.

**The Goal**

For enhanced security, the service instance shall serve as the authenticated endpoint at the application layer.

To achieve this, DT advises a comprehensive study of solutions and their associated implications for repositioning authentication to the application layer.

Such a shift would effectively decouple secure transport/communication from application layer authentication, thereby fostering more secure cloud deployments within a 6G CN.

# 4 Objective

The objective of this WT is to:

* Study the feasibility and potential security implications of moving authentication to the application layer.
* Study and assess possible solutions for application layer authentication.
* …

# 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 |
|  TBD | TBD | TBD | TBD | TBD | TBD |
|  |  |  |  |  |  |

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

# 6 Work item Rapporteur(s)

TBD

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

TBD.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Deutsche Telekom |
|  |
|  |
|  |
|  |
|  |