**3GPP TSG-SA3 Meeting #115 *S3-240680-r1***

**Athens, Greece, 26th February - 1st March 2024** **(revision of xx-yyxxxx)**

**Source: Ericsson, Deutsche Telekom**

**Title: Study on NRF public key retrieval by NF Service Producers**

**Document for: Agreement**

**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 NRF public key retrieval by NF Service Producers

Acronym: FS\_eSBA\_SEC\_Ph2

Unique identifier:

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

Potential target Release: Rel-19

# 1 Impacts

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

# 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 | | | |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
|  |  |  | N/A |

### 2.3 Other related Work Items and dependencies

|  |  |  |
| --- | --- | --- |
| Other related Work /Study Items (if any) | | |
| Unique ID | Title | Nature of relationship |
| 850016 | Security for 5G\_eSBA | Rel-16 work item |
| 900020 | Study on enhanced Security Aspects of the 5G Service Based Architecture | Rel-17/Rel-18 study item |

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

# 3 Justification

According to Step 2 in Clause 13.4.1.1.2 in TS 33.501, an NF Service Producer ensures the integrity of the access token presented by an NF Service Consumer by verifying the signature in the access token using NRF’s public key. However, the current specification does not specify a mechanism for NF Service Producers to retrieve the authentic public key associated with the private key that the NRF has used to produce the signature in the access token.

Currently, the information related to the public keys needed to verify the signature in the access token is assumed to be configured manually at the NFp. Manual configuration does not scale well and is error-prone. This is a concern in large real-world deployments, especially those have layered structured NRFs and use key rotation.

A mechanism for NF Service Producers themselves to obtain the right public keys would be both more efficient and more secure since, e.g., keys can be provisioned and updated more reliably and easily. Such mechanisms are defined for CCA-based authentication by including either the X.509 URL (x5u) or the X.509 Certificate Chain (x5c) in the CCA token. It is not immediate if one of these mechanisms could also work for tokens issued by an NRF or a new solution would be required.

# 4 Objective

The study has the following objective(s):

1. A mechanism for NF Service Producers themselves to retrieve the authentic public key associated with the private key that the NRF has used to produce the signature in the access token.

## TU estimates and dependencies

|  |  |  |  |
| --- | --- | --- | --- |
| Work Task ID | TU Estimate (Study) | TU Estimate (Normative) | Other 3GPP Group Dependency  (Yes/No/Maybe) |
| Objective #1 | 0.75 (0.25 per meeting cycle) | 0.5 (0.25 in each meeting cycle) | No |

**Total TU estimates: 1.25 TU**

**Total TU estimates for the normative phase: 0.5 TU**

**Total TU estimates for the study phase: 0.75 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 NRF public key retrieval by NF Service Producers | TSG#105 (Sept 2024) | TSG#106 (Dec 2024) | TBD |

|  |  |  |  |
| --- | --- | --- | --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} | | | |
| TS/TR No. | Description of change | Target completion plenary# | Remarks |
| 33.501 | Enhancing security aspects of the 5G Service Based Architecture | TSG#107 (Mar 2025) |  |

# 6 Work item Rapporteur(s)

TBD

# 7 Work item leadership

SA WG3

# 8 Aspects that involve other WGs

CT4 for stage 3 work.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Ericsson |
| Deutsche Telekom |
| AT&T |
| Oracle Corporation |