**3GPP TSG-SA3 Meeting #108e *draft\_S3-221864-r1***

**e-meeting, 22 - 26 August 2022**

**Source: Nokia, Nokia Shanghai Bell**

**Title: KI7 solution how to handle static auth in roaming with existing methods**

**Document for: Approval**

**Agenda Item: 5.24**

# 1 Decision/action requested

***Another solution on how to handle static auth with existing methods is presented.***

# 2 References

[1] 3GPP TR 33.875

# 3 Rationale

*Existing stage 3 methods allow to cover the scenario proposed in this key issue and is documented by this solution.*

# 4 Detailed proposal

*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE*

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[3] 3GPP TS 23.501: "System architecture for the 5G System (5GS); Stage 2".

[4] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[5] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3"

[6] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3"

[Y] GSMA NG.113: "5GS Roaming Guidelines"; https://www.gsma.com/newsroom/wp-content/uploads/NG.113-v6.0.pdf

*\*\*\*\*\*\*\*\*\* NEXT CHANGE*

## 6.X Solution #X: Authorization mechanism negotiation using existing methods

### 6.X.1 Introduction

This solution addresses Key Issue #7 "Authorization mechanism negotiation". It is proposed to use the two NRFs for the authorization mechanism negotiation.

### 6.X.2 Solution details

From the oAuth2Required indication that is specified in 29.510, the vNRF can imply, whether OAuth2.0 or static authorization is to be used within one PLMN. This covers the use case, where within one PLMN maybe not yet all NFs use OAuth2.0.

For inter-PLMN stage 3 (TS 29.510 Table 6.1.6.2.3-1) introduced with "oauth2Required" one option to handle the authorization method setting by the hNRF. Another type for NFService, the "perPlmnOauth2ReqList", includes the Oauth2-based authorization requirement supported by the NF Service Instance per PLMN of the NF Service Consumer.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| oauth2Required | boolean | O | 0..1 | It indicates whether the NF Service Instance requires Oauth2-based  authorization.  Absence of this IE means that the NF Service Producer has not provided any indication about its usage of Oauth2 for authorization. |
| perPlmnOauth2ReqList | PlmnOauth2 | O | 0..1 | When present, this IE shall include the Oauth2-based authorization requirement supported by the NF Service Instance per PLMN of the NF Service Consumer.  This IE may be included when the Oauth2.0 authorization requirement supported by the NF Service Instance for different PLMN is different. When the requester PLMN Id is available in perPlmnOauth2ReqList IE, this IE shall override the oauth2Required IE. If the requester PLMN ID is not present in perPlmnOauth2ReqList IE, then the value of oauth2Required IE shall be applicable if available. |

Table Z1: The IEs oauth2Required and perPlmnOauth2ReqList, part of TS 29.510 Table 6.1.6.2.3-1

In addition, stage 3 has specified for inter-PLMN usage the type PlmnOauth2 (see clause 6.1.6.2.102 3GPP TS 29.510 [6]. If the optional attribute "oaut2NotRequiredPlmnIdList" is used, the pre-configured information by HPLMN how to apply static authorization with a specific roaming partner is used.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| oauth2RequiredPlmnIdList | array(PlmnId) | O | 1..N | It shall indicate the consumer PLMN ID list for which NF Service Instance requires Oauth2-based authorization.  (See NOTE 1) |
| oauth2NotRequiredPlmnIdList | array(PlmnId) | O | 1..N | It shall indicate the consumer PLMN ID list for which NF Service Instance does not require Oauth2-based authorization.  (See NOTE 1) |
| NOTE 1:   The same PLMN Id shall not be present in both oauth2RequiredPlmnIdList and oauth2NotRequiredPlmnIdList. | | | | |

GSMA has further provided the following recommendations given in NG.113 [Y], clause 7.6.3.4:

"It is recommended that both VPMN and HPMN use either static authorization or authorization using OAuth2 access token.

Note: Authorization is not possible in case the HPMN only uses authorization using OAuth2 access token and the VPMN only uses static authorization.

If using authorization using OAuth2 access token it is recommended that both VPMN and HPMN support oauth2Required IE as specified in 3GPP Release 16 TS 29.510 [16]. If the HPMN wants to use authorization using Oauth2 only for some VPMNs then HPMN must support perPlmnOauth2ReqList IE as specified in 3GPP Release 17 TS 29.510 [16]."

### 6.X.3 Evaluation

Several means to allow a PLMN's hNRF to provide to the requesting vNRF information on the authorization method used exist in the current specification TS 29.510 [6]. If in the array(PlmanId) of hPLMN NRF a roaming partner is on the "oauth2NotRequiredPlmnIdList", static authorization can be used with this roaming partner. When operators follow the recommendations given in NG.113 [Y], the key issue seems to be covered sufficiently by the existing methods.

*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGE*