**3GPP TSG-SA3 Meeting #108e-AdHoc *draft\_S3-222811-r2***

**e-meeting, 10 - 14 October 2022**

**Source: Nokia, Nokia Shanghai Bell**

**Title: KI7 Sol17 EN resolution**

**Document for: Approval**

**Agenda Item: 5.24**

# 1 Decision/action requested

***EN resolution in solution 17.***

# 2 References

[1] 3GPP TR 33.875

# 3 Rationale

Editor's Note: it is ffs how to solve the case that one operator uses token-based authorization and its roaming partner uses static authorization.

*Needs to be resolved. The following text is added:*

*The solution assumes that discovery is used by both PLMNs according to the standard. Thus, both PLMNs understand the oAuth2Required indication that is specified in 29.510 and can be used during discovery.*

Editor's Note: it is ffs how to configure the NF profile one-by-one, especially when the authorization of one PLMN is changed.

*Needs to be resolved. The following text is added:*

*How to configure the NF profile is out of scope of this solution.*

Editor's Note: Further evaluation is FFS.

*Needs to be resolved. It is proposed to delete this EN. Unclear what further evaluation would be needed.*

# 4 Detailed proposal

\*\*\*\* START OF CHANGES

6.17 Solution #17: Authorization mechanism negotiation using existing methods

6.17.1 Introduction

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

6.17.2 Solution details

The solution assumes that discovery is used by both PLMNs according to the standard. Thus, both PLMNs understand the oAuth2Required indication that is specified in 29.510 and can be used during discovery.

The key issue use case assumption is that one PLMN supports and uses only static authorization but not OAuth2.0. However, this is not in line with TS 33.501 Rel-15 (clause 13.4.1.0), which states: “The authorization framework uses the OAuth 2.0 framework as specified in RFC 6749 [43]. […] The authorization framework described in clause 13.4.1 is mandatory to support for NRF and NF.”

Therefore, this solution follows that at least the support for OAuth2.0 is provided, thus, even if not used finally, the NRF and NFs of a PLMN using only static authorization need to at least understand the attributes as follows.

From the oAuth2Required indication, 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 6.17.2-1: 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 can be used.

NOTE: Stage-3 details can be improved by stating this explicitly or clarify the situation with static authorization.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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. |

Further, the IE ooath2Required used in the bootstrapping is used to indicate whether NRF requires OAuth2 based authorization for accessing its services:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| oauth2Required | map(boolean) | O | 1..N | When present, this IE shall indicate whether the NRF requires Oauth2-based authorization for accessing its services.The key of the map shall be the name of an NRF service, e.g. "nnrf-nfm" or "nnrf-disc".The value of each entry of the map shall be encoded as follows:- true: OAuth2 based authorization is required.- false: OAuth2 based authorization is not required.The absence of this IE means that the NRF has not provided any indication about its usage of Oauth2 for authorization. |

**Table X: oauth2Required for service access from NRF, part of 29.510, see Table 6.4.6.2.2-1: Definition of type BootstrappingInfo**

GSMA has further provided the following recommendations given in NG.113 [8], 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]."

How to configure the NF profile is out of scope of this solution.

6.17.3 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(PlmnId) of hPLMN NRF a roaming partner is on the "oauth2NotRequiredPlmnIdList", static authorization can be used with this roaming partner. However, it is recommended to check stage 3 specification per LS request, whether text clarifications in case of static authorization to be used would provide an improvement for addressing the use case of this key issue.

When operators follow the recommendations given in NG.113 [8], the key issue seems to be covered sufficiently by using the existing methods.

\*\*\*\* END OF CHANGES