**3GPP TSG-SA3 Meeting #108e-AdHoc *draft\_S3-222811-r3***

**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

5.7 Key issue #7: Authorization mechanism determination

5.7.1 Key issue details

It is specified in TS 33.501 [2] clause 13.3.0 that static authorization can be used for authorization when token-based authorization is not used. However, two PLMNs may have a roaming issue if the authorization mechanism is not aligned between them. For example, when the NF Service Consumer (NFc) deployed in one PLMN only uses static authorization, and the NF Service Producer (NFp) deployed in the other PLMN only uses OAuth authorization, the NFp will reject the NF Service Consumer.

TS 29.510 [6] defined an oauth2Required indicating whether OAuth authorization is required for the NFp service access, which is sent back to the NFc via the discovery response. Accordingly, NFc should get the OAuth token before consuming the NFp services, if the indication is set to true. Hence, an NFc that only uses static authorization, will not be able to consume the service provided by the NFp.

The key issue will investigate solutions allowing the two operators to handle the case that one operator uses token-based authorization and its roaming partner uses static authorization. The failure issues when the NFc only uses static authorization should be clarified.

5.7.2 Security threats

The SBA service authorization will fail in the roaming case if the authorization mechanism is not aligned between them.

5.7.3 Potential security requirements

The 5GS should provide mechanisms to handle the case that one operator uses token-based authorization, and its roaming partner uses static authorization.

\*\*\*\* NEXT CHANGE

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 are able to understand the OAuth2Required indication as specified in 29.510 when NRFs communicate with each other, and when a NF service is discovered at NRF.

The key issue use case assumption is that one PLMN uses only static authorization.Based on TS 33.501 Rel-15 (clause 13.4.1.0): “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.” and clause 13.4.0, static authorization can be used. “It can be used when token-based authorization is not used.”

This solution follows the standard, i.e. that at least the support for OAuth2.0 is provided, thus, even if not used, NRF and NFs of a PLMN using only static authorization need to at least understand the attributes (IEs) provided during discovery.

This solution suggests that 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) "oauth2Required" can be used to handle the authorization method setting by the hNRF. Another type for NFService, the "perPlmnOauth2ReqList", is also specified and 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 solution suggests that in this case pre-configured information by HPLMN (how to apply static authorization with a specific roaming partner) can be used.

Stage-3 details could be improved by stating explicitly that oauth2NotRequired refers to 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 oauth2Required used in the bootstrapping information 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**

If set to false, OAuth2 based authorization is not required. This solution proposes to clarify stage 3 that this mean, the only other available authorization mechanism “static authorization” is the default in this case.

GSMA has 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 in case the operator wants to change to another authorization method is out of scope of this solution. By OAM this could be automated for each NF affected.

If the operator of one PLMN does not want to follow the specification and only supports static authorization, and the other operator requires the usage of OAuth, then in a consequence, those operators cannot have a roaming agreement. The service request has to be rejected if one PLMN does not accept a request without an OAuth token.

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] and are provided for information by this solution. If in the array(PlmnId) of hPLMN NRF a roaming partner is on this "oauth2NotRequiredPlmnIdList", the solution proposes that this says implicitly which PLMN Ids use static authorization .

When operators follow the recommendations given in NG.113 [8], the key issue seems to be covered sufficiently by using the existing methods. However, stage 3 specification could benefit from a text clarification along the lines of this solution to cover the case of static authorization to be used by one operator, but not by the other and how to handle the error case.

\*\*\*\* END OF CHANGES