**3GPP TSG-SA5 Meeting #156 *S5-244308***

**Maastricht, Netherlands, 19th Aug 2024 - 23rd Aug 2024**

**Source: Nokia**

**Title: Rel-19 pCR TR 28.879 Evaluation analysis for authorization of the external MnS consumer to access the management service API use case**

**Document for: Approval**

**Agenda Item: 6.19.21**

# 1 Decision/action requested

***In this box give a very clear / short /concise statement of what is wanted.***

# 2 References

[1] 3GPP TR 28.879, " Study on OAM for service management and exposure to external consumers".

# 3 Rationale

This pCR proposes to add an evaluation analysis for the authorization of the external MnS consumer to access the management service API use case in clause 5.1.4 of TR 28.879 [1].

# 4 Detailed proposal

It is proposed that the following changes be made in clause 5.1.4 of TR 28.879 [1].

|  |
| --- |
| **First 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 28.533: “Management and orchestration; Architecture Framework”.

[3] 3GPP TS 28.622: “Telecommunication management; Generic Network Resource Model (NRM) Integration Reference Point (IRP); Information Service (IS)”

[4] 3GPP TS 28.537: “Management and orchestration; Management capabilities”.

[5] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2"

[6] SP-231669: "LS on collaboration and alignment of 3GPP defined application enablers with GSMA Open Gateway".

[7] 3GPP TS 23.434: "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows".

[8] 3GPP TS 23.255: "Application layer support for Vehicle-to-Everything (V2X) services; Functional architecture and information flows".

[9] 3GPP TS 23.286: "Application layer support for Uncrewed Aerial Systems (UAS) services; Functional architecture and information flows".

[10] 3GPP TS 23.545: "Application layer support for Factories of the Future (FF) ".

[11] 3GPP TS 23.542: "Application layer support for Personal IoT Networks".

[12] 3GPP TS 23.554: "Application architecture for MSGin5G Service; Stage 2".

[13] 3GPP TS 29.222: "Common API Framework for 3GPP Northbound APIs; stage 3".

[14] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP Northbound APIs".

[15] "The Ecosystem for Open Gateway NaaS API Development", white paper, June 2023 [[link](https://www.gsma.com/solutions-and-impact/gsma-open-gateway/wp-content/uploads/2023/05/The-Ecosystem-for-Open-Gateway-NaaS-API-development.pdf)]

[16] "GSMA Operator Platform Group – Requirements and Architecture", version 5.0, July 2023 [[link](https://www.gsma.com/futurenetworks/wp-content/uploads/2023/07/OPG.02-v5.0-Operator-Platform-Requirements-and-Architecture.pdf)]

[17] 3GPP TS 28.532: "Management and orchestration; Generic management services".

[18] 3GPP TS 28.531: "Management and orchestration; Provisioning"

[19] 3GPP TS 23.435: "Procedures for Network Slice Capability Exposure for Application Layer Enablement Service"

[20] 3GPP TS 23.558: "Architecture for enabling Edge Applications"

[21] 3GPP TS 28.550: "Management and orchestration; Performance assurance"

[22] 3GPP TS 28.111: "Management and orchestration; Fault Management (FM)"

[23] 3GPP TS 28.105: "Management and orchestration; Artificial Intelligence / Machine Learning (AI/ML) management"

[24] 3GPP TS 28.104: "Management and orchestration; Management Data Analytics (MDA)"

[25] 3GPP TS 28.541: "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and 3"

[26] 3GPP TS 28.312: "Management and orchestration; Intent driven management services for mobile networks"

[27] 3GPP TS 28.538: "Management and orchestration; Edge Computing Management"

[28] 3GPP TS 28.536: "Management and orchestration; Management services for communication service assurance; Stage 2 and 3"

[29] 3GPP TS 28.319: “Management and orchestration; Access control for management services”

[30] 3GPP TS 32.158: " Management and orchestration;Design rules for REpresentational State Transfer (REST) Solution Sets (SS)”.

[31] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

 [32] IETF RFC 7519: “JSON Web Token (JWT)”.

|  |
| --- |
| **Second Change** |

#### 5.1.4.3 Potential solutions

###### 5.1.4.3.i.1 Introduction

Editor's Note: This clause describes briefly the potential solution at a high-level.

###### 5.1.4.3.i.2 Description

Editor's Note: This clause further details the potential solution and any assumptions made.

#### 5.1.4.4 Evaluation of potential solutions

The proposed solution covers the requirement **PREQ-FS\_MExpo-Auth-01** of the use case. However, the proposed solution has the following limitations when it comes OAuth2.0 scopes:

1. Given that the access token is carried in the HTTP authorization header (see RFC 6750[31]), size limitations are introduced on how big the access token could be. In the 3GPP management system, the access control for each MnS consumer is at the granularity of the resources (i.e., MOIs, IOCs, or their corresponding attributes), the operations that can be performed on these resources, and the actions that are allowed on the permitted operations. This implies that as the number of resources the external MnS consumer is authorized to access increases, so does the size of the access token since the access rule(s) are stored in the "scope" attribute of the access token.
2. At the MnS producer, as the enforcer, the MnS producer is incharge of validating the access token provided by the external MnS consumer (see clause C.7 TS 33.122[14]). The validation process of the access token involves ensuring that the access token is a valid (see RFC 7519[32]). Upon validation, the MnS producer needs to map the scope value of the access token to the access rules (see clause C.5 TS 33.122[14]) and ensure that the access rules are valid for the external MnS consumer. To do this, the MnS producer can contact the authorization server. These checks (i.e., the access token validation, the mapping and the validation of the access rules applicable to the external MnS consumer) contribute to the processing time of the access token on the MnS producer.

|  |
| --- |
| **End of Changes** |