**3GPP TSG-SA5 Meeting #158 *S5-247134***

Orlando, USA, 18 - 22 November 2024

**Source: Nokia, Samsung**

**Title: DP on authorization of the external MnS consumer to consume management services at the CCF**

**Document for: Endorsement**

**Agenda Item: 6.19.21**

# 1 Decision/action requested

***The group is asked to discuss and endorse the proposal.***

# 2 References

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

[2] 3GPP TS 28.319: "Management and orchestration; Access Control for Management services".

# 3 Rationale

Clause 5.4.1 of TR 28.879 describes how to authorize an external MnS consumer to access the management service API without describing exactly how the authorization information for a specific external MnS consumer will be made available at the CCF. According to the CAPIF specifications, the CCF shall be enabled to generate the access token for an external MnS consumer (referred to as API invoker in CAPIF terms) to invoke service APIs. However, how the CCF will be enabled to generate access tokens for external MnS consumers at run-time is still not described.

This contribution aims to propose a potential solution enabling the CCF to provide authorization information to external MnS consumers to invoke service APIs.

## 3.1 Proposed solution for CCF authorization of an external MnS consumer to invoke service APIs

### 3.1.1 Using AccessRule to configure authorization information.

The potential solution assumes that the network operator has a portal with a list of services APIs and the corresponding metadata providing the external MnS consumer with the option to choose what service APIs they would like to subscribe to. Such functionality is provided offline and not subject to standardization.

After the external MnS consumer has identified the service APIs they would like to subscribe to, the CAPIF API invoker enrolment phase can start (refer to clause 5.1.3). This solution assumes that the 3GPP management system can define which AccessRule(s) and Role(s) are appropriate for the external MnS consumer, based on the list of service APIs that the external MnS consumer would like to enrol for. Accordingly, as part of the enrolment phase the 3GPP management system administrator does the following:

* Creates new AccessRule(s); if no existing access rules apply for the external MnS consumer, that will govern the interactions with the granted service API(s).
* Creates a new Role(s) to associate with the newly created AccessRule(s) or associates an existing Role with the external MnS consumer.
* Create an MSAC Identity associated with the external MnS consumer and assigns the associated Role(s). The created MSAC Identity instance holds the authorization information of the external MnS consumer in the MSED.

These data are stored in the authentication and authorization MnS producer.

Subsequently, when generating the CAPIF enrolment details (e.g., CCF URL and CCF security information) for the external MnS consumer, the authentication and authorization MnS producer also generates the onboarding access token to enable the CAPIF onboarding procedure. Finally, the authentication and authorization MnS producer maintains a mapping between the assigned MSAC Identity for the external MnS consumer and the generated onboarding access token. The MSED is responsible for sending the enrolment onboarding information (i.e., the CCF details (URL, Root CA certificate)) to the external MnS consumer. The enrolment procedure is done offline and not subject to standardization.

### 3.1.2 Potential solution #x: Identity class made available to the CCF

#### 3.1.2.1 Introduction

From the 3GPP management system perspective, the Identity class represents information that can be made available to any access control system. The Role class is associated to one or more access rules based on the AccessRule class whose notation is specific to the 3GPP management system (see TS 28.319[2]).

In this regard, the MSAC information that is eligible to be provided to the CCF is limited to the MSAC Identities associated to the different API invokers/external MnS consumers.

#### 3.1.2.2 Description

From clause 3.1.1, the MSAC identity and generated onboarding access token for an external MnS consumer is known by the authentication and authorization MnS producer. The potential solution focuses on how to make authorization information for an external MnS consumer available in the CCF as shown in Figure 3.1.2.2-1.

A screenshot of a computer

Description automatically generated

Figure 3.1.2.2-1: External MnS consumer authorization by the CCF

1. To begin the onboarding procedure, the API invoker establishes a secure connection with the CCF based on TLS server-side authentication. The server certificate is CCF’s Root CA, which was sent to the API invoker after enrolment (see step 6 in clause 5.1.4.3.1.2).
2. The API invoker sends an onboard API invoker request to the CCF over the CAPIF-1/CAPIF-1e interface. This request involves providing the onboarding enrolment information using the “APIInvokerEnrolmentDetails” data type (see clause 8.4.4.2.2 of TS 29.222[13]). This data type includes the onboarding credential, which was sent to the API invoker after enrolment (see step 6 in clause 5.1.4.3.1.2).
3. The CCF sends an acknowledgment for receiving the onboard API invoker request to the API invoker.
4. The CCF takes the “onboarding credential” from the APIInvokerEnrolmentDetails data type, and sends it to the Authentication and authorization MnS producer
5. The Authentication and authorization MnS producer validates the received “onboarding credential”.
6. If the “onboarding credential” is valid, the Authentication and authorization MnS producer retrieves the MSAC identity instance associated to the onboarding credential (see step 4 of clause 5.1.4.3.1.2). The retrieved Identity instance represents the authorization information of the API invoker.
7. The Authentication and authorization MnS producer sends the associated MSAC identity for the API invoker to the CCF.
8. Upon receiving the associated MSAC identity, the CCF generates API invoker id that represents a unique identifier for the API invoker in the CCF. The CCF associates the generated API invoker id with the received MSAC identity.
9. The CCF sends an onboard API invoker response to the API invoker with the response body represented by the “APIInvokerEnrolmentDetails” data type. The response includes the assigned API invoker ID

To gain access to one or more service APIs, the API invoker needs to get authorized using CAPIF built-in OAuth2.0 framework. As described in clause 6.5.2.3 of TS 33.122 [14, this authorization procedure is a two-stage process, i.e., Service API invocation authorization request (steps 10 - 16) and service API invocation.

1. When the API invoker wants to invoke specific service APIs, it establishes a TLS session with the CCF based on certificate-based mutual authentication.
2. The API invoker sends an access token request to the CCF to invoke specific service API(s) providing the API invoker id and optionally a list of service API(s) it wants to invoke. The request body carries the information described by the AccessTokenReq data type (clause 8.5.4.2.6 of TS 29.222[13]).
3. The CCF validates the request, and if valid, retrieves the MSAC Identity associated to the API-invoker-id” (see step 9). This API-invoker-id is in the “client\_id” parameter of the received access token request.
4. The CCF sends access token request to the Authentication and authorization MnS producer. In this request, the “client\_id” of the access token request is set to the associated MSAC Identity of the API invoker (retrieved in step 12).
5. The Authentication and authorization MnS producer validates the request and generates an access token. This token will contain, as part of token claims, the allowed APIs (MnSes) that the API invoker is authorized to invoke.
6. The Authentication and authorization MnS producer sends the generated access token to the CCF.
7. Upon receiving the access token, the CCF forwards the received access token response to the API invoker. The CCF sends a "service API authorization response", which carries the information described by the AccessTokenRsp data type.
8. Subsequently, the API invoker can successfully invoke the service API at the AEF as described in clause 6.5.2.3 of TS 33.122[14].

NOTE: How the CCF interacts with Authentication and authorization MnS producer is up to implementation and not subject to standardization. The implementation may choose to collocate or not the CCF and the authentication and authorization MnS producer

# 4 Detailed proposal

It is proposed to endorse the solutions described in clauses 3.1.1 and 3.1.2 to enable the authorization of external MnS consumers to invoke service API at the CCF.