**3GPP TSG-SA5 Meeting #156 *S5-244746d2***

Maastricht, The Netherlands 19 - 23 August 2024

**Source: Huawei**

**Title: pCR TR 28.879 Update concepts**

**Document for: Approval**

**Agenda Item: 6.19.21**

# 1 Decision/action requested

***Group is asked to approve this proposal.***

# 2 References

[1] 3GPP TS 28.879 Study on OAM for service management and exposure to external consumers

# 3 Rationale

This contribution elaborates the following concept and background information which are related to management service exposure.

1. Add the description of using access control in Overview clause.
2. Add more existing SA5 solutions related to exposure.
3. Update the example of external consumer diagram.

# 4 Detailed proposal

*It’s proposed to make the following change to TR 28.879.*

# 4 Concepts and Background

## 4.1 Exposure of management services

### 4.1.1 Overview

The present document studies a generic approach to expose management services to external MnS consumers. A management service (MnS) is identified by different component types, i.e., MnS component type A (management operations or notifications), MnS component type B (managed objects), and MnS component type C (performance and fault information) (as defined in clause 4.2 of TS 28.533 [2]). Accordingly, in order for the external MnS consumer to consume management services, the access rights have to be configured for the external MnS consumer. These access rights determine which MnS resources (i.e. component type B and component type C) can be accessed. In addition, the access rights also determine what operations (i.e. MnS component A) can or cannot be performed on the MnS resources. For example, considering Figure 4.1.1-1, the MnS A producer produces MnS A that is directly consumed by the internal MnS consumer and the external MnS consumers 1 and 2 respectively. Depending on the different access rights assigned to the external MnS consumers 1 and 2, it’s possible that:

- The internal MnS Consumer and external MnS Consumer 1 and 2 can access the same or different managed objects under the management scope of MnS A producer.

- The operations (i.e., CRUD) or notifications that internal MnS Consumer and external MnS Consumer 1 and 2 can perform on the accessed managed objects are the same or different.

- The internal MnS Consumer and external MnS Consumer 1 and 2 can or cannot access the same or different performance and fault information associated with the accessible managed objects of MnS A.



Figure 4.1.1-1: Example of Exposing Management Services concept.

To provide a MnS to be consumed, it first needs to be published to the MnS discovery producer entity. After it’s published, the MnS will be available to be discovered by the external MnS consumers. Following discovery, authentication and authorization mechanisms need to be applied to ensure that the external MnS consumers only have access to the allowed MnS component type A, B, or C for the MnS.

### 4.1.2 Background of existing SA5 solutions related to exposure

In the study, we will focus on how the external MnS consumer can leverage external exposure frameworks (e.g., the CAPIF framework [5]) to access and consume management services with regards to all the stages involved: publishing of new MnS, discovery of MnS and access control for MnS.

A MnS can be available (i.e., instantiated, and ready to be exposed) and hence discoverable by internal and external MnS consumers using 3GPP standard as defined in following specifications:

- An available MnS is described by the MnsInfo IOC (see clause 4.3.42 of TS 28.622 [3]).

- The available MnSs in the 3GPP management system can be found in the MnSRegistry IOC (see clause 4.3.41 of TS 28.622 [3])

- The use case procedures for discovery are described in clause 5 of TS 28.537 [4].

The access control framework is defined in TS 28.319 [29]:

- The concept and solution for access control are described in clause 4 and clause 7 of TS 28.319 [29].

### 4.1.3 Background on existing telco exposure initiatives

#### 4.1.3.1 3GPP exposure framework

3GPP standard exposure technologies hide the complexity of 5G and offer 3rd party applications a simple, secure, use-case-oriented configuration interface to the 5G system. The exposure interfaces will be quite valuable to a multitude of industrial use cases (i.e., non-telco use cases, with requirements beyond secure and reliable connectivity), allowing industry verticals to make use of the key features and performance that 5G has to offer in a simple and straightforward manner.

The development of solutions for exposure in 3GPP is led by SA6 WG. Figure 4.1.3.1-1 pictures the latest status of the 3GPP exposure framework. As seen, the framework consists of a set of Application Enablement Services ("Edge", "SEAL", "Vertical App Enabler") that pursue one mission: to provide means to 3rd parties to rapidly develop and deploy new vertical-oriented applications ("Application Layer") over 3GPP system ("Network and OAM/CH"). To that end, Application Enablement services offer industry-tailored APIs ("Northbound Interface – service APIs") that build on 3GPP system APIs ("Southbound Interface – network APIs"). All these APIs are documented in 3GPP Technical Specifications and made available under the 3GPP GitLab repository.



Figure 4.1.3.1-1: 3GPP exposure framework (Figure extracted from [6]).

SA6 WG realized soon that managing all these APIs, especially in an environment where 3rd parties are developing applications, will also require a management layer that enforces the strong security policies defined by SA3 WG (e.g., Mutual TLS Authentication). This is where "CAPIF" comes to the picture. Common API Framework (CAPIF) is defined to manage access to all 3GPP APIs, in a consistent and uniform way with regards to publication, discovery and access control, among other functionalities. The operator can use CAPIF as an entry point for the Application Layer to gain access to 3GPP APIs, including not only the APIs offered by Application Enablement services (SA6), but also the APIs offered by the 3GPP system (SA2 and SA5).

Table 4.1.3.1-1 provides a more detailed description of all the components mentioned above.

Table 4.1.3.1-1: Components of the 3GPP exposure framework

|  |  |
| --- | --- |
| **Component** | **Description** |
| 3GPP system | Also referred to “5G Network Services” in Figure 4.1.3.1-1, it includes:- Network Services: groups all the capabilities related to 3GPP SA2. These are made available through Core network functions, e.g. Network Exposure Function (NEF).- OAM/CH services: groups all the capabilities related to 3GPP SA5. These capabilities are offered through MnSs by producers.  |
| Edge Services | It includes services for hosting edge computing applications, while consolidating edge computing standardization in 3GPP. These services provide various capabilities such as rich discovery of the edge application servers (EAS), service continuity between multiple edge data networks (EDN), interworking with the core network, and APIs for EASs to integrate with the edge hosting environments. The main components building out this layer are specified in TS 23.558 [20]:- Edge Enabler Server (EES), primarily responsible for enabling discovery of EASs.- Edge Enabler Client (EEC), providing support functions, such as EAS discovery to the application clients in the device. - Edge Configuration Server (ECS), providing configurations to the EEC to connect with targeted EAS(s).Note that the Edge Computing Layer only consumes network capability set from the 3GPP system (see Figure 4.1.3.1-1) |
| Service Enabler Abstraction Layer (SEAL) | It provides a set of core services that are common to industry verticals. The motivation is largely to avoid redefining the individual services for each vertical industry, thereby lowering the deployment costs for operators, and significantly reducing the barrier of adoption and the time-to-market for integrating new verticals to the 3GPP ecosystem. SEAL services are specified in TS 23.434 [7], and include location management, group management, configuration management, identity management, key management, network resource management, data delivery, notification management, network slice capability enablement (NSCE) and application data analytics enablement |
| Vertical App Enabler (VAE) | It provides vertical-specific service enablers. In contrast to the SEAL, VAE targets service specific vertical applications. As of today, the verticals service enablers are defined for:- automotive applications referred to as vehicle-to-anything (V2X) communications, see TS 23.255 [8].- drone applications known as uncrewed aerial systems (UAS), see TS 23.286 [9]- Industry 4.0/OT applications, also referred to as factories of the future (FF), see TS 23.545 [10]- Personal IoT networks, see TS 23.542 [11]- Message communication in massive IoT, also referred to as MSGIn5G, see TS 23.554 [12]. |
| Common API Framework (CAPIF) | Started in Release 15, CAPIF services are listed in TS 23.222 [5] and specified in TS 29.222 [13] with security aspects being addressed in TS 33.122 [14]. It provides a unified Northbound API framework across network/application functions, to facilitate a harmonized approach for API exposure within 3GPP. This framework builds upon three main components:- API invokers: they represent consumers of 3GPP APIs. - CAPIF Core Function (CCF): responsible for managing onboarding of API invokers, and access control (authentication, authorization) when trying to gain access to 3GPP APIs. - API provider domain: collection of functions (discovery, registration, publishing, auditability) required to allow authorized API invokers to consume 3GPP APIs. They implement agents that allow API producers to make APIs available through CAPIF.  |
| Application Layer | This layer represents the 3rd party applications that want to gain access (discover and consume) 3GPP APIs, to develop and deploy new vertical services.  |

#### 4.1.3.2 GSMA Open Gateway

The development of telco capability exposure (also coined “Network as a Service”, NaaS) requires a collaborative workspace that bring together incumbent telco standard bodies with IT/cloud communities, industry associations and open-source projects. An effective collaboration among organizations needs to be based on a clear demarcation on their scope of work, avoiding their participating organizations running overlapping activities or duplicate efforts; otherwise, NaaS may risk ending up with a fragmented ecosystem. To that end, the GSM Association (GSMA) launched Open Gateway in MWC Barcelona 23. GSMA Open Gateway mission is twofold:

i) to provide a governance framework for NaaS, covering technical and business aspects;

ii) to get operator commitment to launch universal NaaS API services in 2023.

Open Gateway initiative recognizes that NaaS the concept builds on the work developed by three organizations – see Table 4.1.3.2-1. The role of the different organizations and their relationship is graphically shown in Figure 4.1.3.2-1.

Table 4.1.3.2-1: Organizations participating in GSMA Open Gateway initiative.

|  |  |
| --- | --- |
| **Organization** | **Description of Activity** |
| Linux Foundation’s CAMARA | it represents the “exposure” doctrine, i.e., how capabilities are exposed for external consumption through 3rd party facing APIs. CAMARA defines these APIs and is responsible for their hosting and release management. 3rd party facing APIs are dev-friendly (semantics tailored to service and business needs of 3rd parties) and open (following Apache2.0 license).  |
| GSMA | it represents i) the “technical” doctrine, by specifying how 3rd party facing APIs are to be supported by underlying telco capabilities; and ii) the “business” doctrine, with the definition of agreement templates for federation between the operator networks and for relationship with 3rd parties, ensuring a consistent yet fair commercial framework for exposing services. GSMA conducts the technical workstream through OPG/OPAG (Operator Platform Group / Operator Platform API Group) and the business workstream through WAS (Wholesale Agreement Services) group. |
| TM Forum | it represents the “operational” doctrine, i.e., how 3rd party facing APIs are to be operated and managed, to make a commercial product out of them. Aspects such as 3rd party onboarding, application registration, access control and billing aspects are in scope.  |

On the one hand, scope of “GSMA” is restricted to the telco domain. GSMA prescribes the capabilities that all operators must make available for 3rd parties, to ensure global reach and scale. These must-be capabilities are referred to as Open Gateway services. The GSMA is also responsible for

i) the prioritization and roadmap management of Open Gateway services, according to market needs and commercial readiness of underlying technologies; and

ii) architecting the platform that individual operators will use to realize, federate, and expose Open Gateway services.

On the other hand, the focus of “CAMARA” and “TM Forum is on the dev-friendly APIs that allows programmatic access to Open Gateway services. As seen in the bottom of Figure 4.1.3.2-1, these APIs can be clustered into three groups: service APIs, service management APIs and operate APIs. For further information on these APIs, see [15].

Each Communication Service Provider (CSP) exposes APIs through the Open Gateway Transformation Function (Figure 4.1.3.2-1). Deployed as an internal component of GSMA Operator Platform [16] the Open Gateway Transformation Function is tasked with defining and enforcing the mapping between the dev-friendly APIs (towards 3rd party applications) and network APIs (towards 3GPP system). The mapping logic is not standardized, though GSMA provide non-prescriptive guidelines on a per API basis. For the interaction with OAM systems, the white paper in [15] notes that transformation function may interact with TM Forum (Open API portfolio) and 3GPP SA5 (management services).



Figure 4.1.3.2-1: GSMA Open Gateway ecosystem.

### 4.1.4 Examples of external MnS consumers

Figure 4.1.4-1 provides examples of functional entities that can become external MnS consumers. Table 4.1.4-1 elaborates on the rationale.



Figure 4.1.4-1: Examples of external MnS consumers.

`

Table 4.1.4-1: Examples of external MnS consumers.

|  |  |
| --- | --- |
| **Functional Entity** | **Justification** |
| Application Layer Server | Any 3rd party application that gains access (discover and consume) to MnSs using a discovery mechanism defined outside SA5 is an external MnS consumer. The logic of this application is on the 3rd party and outside standardization.  |
| SEAL’s NSCE server | Network Slice Capability Enablement (NSCE) is a SEAL service that provides add-on slicing capabilities to vertical customers’ applications. NSCE has a server and multiple clients (installed on vertical customer’s devices). NSCE server consumes slicing capabilities related to OAM (i.e., MnSs) and 5G network services (i.e., NEF APIs, NWDAF APIs, NSACF APIs), and process them (aggregation, abstraction, filtering, etc.) in order to build vertical-oriented slicing functionality to applications. The set of operations/notifications related to OAM that are eligible for consumption by NSCE server are specified in TS 28.531 [18], and conceptually grouped under the NSCE-OAM interface in TS 23.435 [19]. To gain access to these capabilities, NSCE server can use a discovery mechanism defined outside SA5. In this regard, the NSCE server becomes an external (network slice / network slice subnet) MnS consumer. |
| Open Gateway Transformation Function | Open Gateway services (defined by GSMA) are offered through dev-friendly APIs (specified and maintained by CAMARA and TM Forum). Some services provisioning and monitoring actions on 5G managed resources, including network slicing. In such a case, the invocation of these dev-friendly APIs needs to be mapped into one or more calls to MnSs. The Open Gateway Transformation Function is in charge of this mapping and MnS invocation. To that end, the Open Gateway Transformation needs to be able to discover MnS. In this regard, one can realize that the Open Gateway Transformation Function complies with the external MnS consumer when it gains access to MnSs using a discovery mechanism defined outside SA5. |

It is worth noting that the functional entities represented as examples of external MnS consumers:

- provides a non-exhaustive list; the only aim is to provide clarity on how external MnS consumer concept fits with the background of telco exposure initiatives reported in the background.

- are all optional; the decision to deploy these functional entities or not is up to operator discretion.

- perform the role of “API invokers”, when the discovery mechanism these entities use to gain access to MnSs is the mechanism provided by CAPIF.