**3GPP TSG-SA WG6 Meeting #68 S6-253510**

**Gothenburg, Sweden 25th – 29th August 2025 (revision of S6-253367)**

**Source: Samsung**

**Title: Pseudo-CR KI on enhancing CAPIF Administrator**

**Spec: 3GPP TR 23.700-43 V0.0.0**

**Agenda item: 9.11**

**Document for: Approval**

**Contact: Basavaraj (Basu) Pattan, basavarajjp@samsung.com**

**1. Introduction**

This pCR proposes KI on enhancements required to the role of CAPIF administrator.

**2. Reason for Change**

CAPIF\_Ph4 SID identifies that currently in TS 23.222 there is limited support for CAPIF administrator role. Further, it states that study is required on whether and how the role of CAPIF administrator can be expanded to consider more practical use cases emerging from the CAPIF deployments.

API provider administrator plays a pivotal role (leveraging API management function) in managing and overseeing the CAPIF operations, ensuring smooth deployment, maintenance, and updates, and monitoring performance to meet service level agreements (SLAs). As an API provider administrator, tracking and analyzing API usage is crucial for ensuring optimal performance, security, and user satisfaction.

This pCR proposes to study the gaps that need to be covered for enabling the API provider administrator to perform responsibilities that are required as per the emerging trends.

Here are some key types of API analytics that would be useful for an API provider administrator and their applications:

1. Usage Metrics

* Requests per Second (RPS): Monitor the number of API requests to identify peak usage times and ensure the system can handle the load.
* Total Requests: Track the overall number of API calls to understand user engagement and growth trends.
* Response Times: Measure the time taken to process requests, helping to identify performance bottlenecks.

2. Error Tracking

* Error Rates: Monitor the frequency of errors (e.g., 4xx client errors, 5xx server errors) to quickly address issues and improve reliability.
* Error Types: Categorize errors to understand common problems and prioritize fixes.

3. User Behavior Analysis

* Most Used Endpoints: Identify which API endpoints are most frequently accessed to optimize resources and focus on high-demand features.
* User Segmentation: Analyze usage patterns by different user groups (e.g., developers, internal teams) to tailor support and documentation.

4. Security Monitoring

* Unauthorized Access Attempts: Detect and log attempts to access unauthorized endpoints or resources.
* Rate Limiting Violations: Track instances where users exceed rate limits to prevent abuse and ensure fair usage.
* Anamoly behaviour: Detect of anomalies in the usage of service APIs.

5. Performance Optimization

* Latency Analysis: Identify slow endpoints and optimize them for faster response times.
* Throughput Analysis: Measure the system's ability to handle concurrent requests and scale accordingly.

6. Business Insights

* Revenue Impact: For monetized APIs, track usage to calculate revenue and assess the financial impact of different features.
* Customer Satisfaction: Use feedback and usage patterns to improve API offerings and enhance user experience.

7. Compliance and Auditing

* Data Usage Reports: Ensure compliance with data protection regulations by monitoring how data is accessed and used.
* Audit Logs: Maintain detailed logs of API activity for auditing purposes and to investigate potential security incidents.

How These Analytics Are Useful:

* Proactive Problem Solving: Early detection of issues allows for quick resolution, minimizing downtime and user frustration.
* Resource Allocation: Insights into usage patterns help allocate resources efficiently, ensuring high availability and performance.
* Security Enhancement: Monitoring for suspicious activities helps in identifying potential threats and implementing necessary security measures.
* Business Growth: Understanding user behavior and preferences aids in developing new features and services that align with market demands.
* Cost Management: Optimizing API performance reduces operational costs by minimizing resource wastage and improving efficiency.

**3. Proposal**

It is proposed to agree the following changes to 3GPP TR 23.700-43 V0.0.0.

\* \* \* First Change \* \* \* \*

# X Key issues

## X.1 Key issue #X: Enhancements to API provider administrator role

### X.1.1 Description

3GPP SA1 has specified the service requirements for exposure in 3GPP TS 22.261 including service exposure, information exposure, etc. And 3GPP SA6 has already specified many APIs in various SEAL specifications, EDGEAPP specification etc. And 3GPP SA6 has defined CAPIF as a framework to support the management of such APIs exposure.

**API provider administrator:** An authorized user with special permissions for the API provider to perform administration of the service APIs.

Below updated definition for API management function in 3GPP TS 23.222 shows the relationship of the API provider administrator and the API management function:

**API management function:** The entity which enables **the API provider administrator at** the API provider to perform administration **(e.g. minimizing downtime, ensuring high availability and performance, identifying potential threats)** of the service APIs.

API provider administrator plays a pivotal role (leveraging API management function) in managing and overseeing the CAPIF operations, ensuring smooth deployment, maintenance, and updates, and monitoring performance to meet service level agreements (SLAs). As an API provider administrator, tracking and analyzing API usage is crucial for ensuring optimal performance, security, and user satisfaction. However, currently in the CAPIF TS 23.222 there is limited support for administrator role via API management function. That is, API management function can Monitor service API invocation and Query service API log for auditing purpose. Hence, going by emerging trends the current support to administrator needs enhancement e.g. via analytics data.

Some key types of API analytics that would be useful for an API provider administrator are Usage Metrics, Error Tracking, User Behavior Analysis, Security Monitoring, Performance Optimization, Business Insights, Compliance and Auditing.

By leveraging these analytics, API provider administrators can ensure that their APIs are reliable, secure, and aligned with business objectives.

### X.1.2 Open issues

To support the enhancements to API administrator role, the following aspects need to be studied:

- What are the key types of API analytics that would be useful for an API provider administrator?

- How to support API analytics at the CAPIF core function?

- How to provide API analyticsto the API management function?