CAPIF SEAL API

# Standardization of Frameworks for Industrial Application Enablement in 3GPP

Core Network Development Department Yuji Suzuki

In recent years, the use of mobile networks in various industries such as automated driving, drones and smart factories has been attracting attention. 3GPP TSG SA WG6 is investigating solutions to enable a variety of industrial applications to take advantage of 3GPP networks. In particular, CAPIF, introduced in Release 15, and SEAL, introduced in Release 16, are anticipated to become service frameworks that can be commonly used in many industries. This article provides an overview of the activities of 3GPP TSG SA WG6 and describes the technical specifications of CAPIF and SEAL.

## 1. Introduction

Mobile network usage is expected across a wider variety of industrial fields as well as telecommunications thanks to technological advancements including, for example, the introduction of the 5th Generation mobile communications system (5G) that delivers high speed/capacity, low-latency and massive connectivity, the development of the Internet of Things (IoT) technology and the digitization of various industrial fields. In the 3rd Generation Partnership Project (3GPP), the technical specifications have been enhanced with a view to cooperating with applications outside the 3GPP domain, as exemplified by the exposure of network capabilities by the Application Programming Interfaces (APIs)[*1] of the Service Capability Exposure Function (SCEF)[*2] and the Network Exposure Function (NEF)[*3].

3GPP TSG SA WG6 (hereinafter referred to as "SA6") has traditionally focused on solutions for mission-critical[*4] communications. In addition, since

[*1] API: An interface for applications to use a specific service. In this article, it refers specifically to the RESTful API.

[*2] SCEF: A logical node that exposes some of the capabilities of the 3GPP system to the outside of the 3GPP domain. It is mainly used in core networks (see *13) for 4G.

[*3] NEF: Similar to SCEF, a functional part of the 5G core network (see *13) that exposes some of the capabilities of the 3GPP system to the outside of the 3GPP domain.

[*4] Mission-critical: A system that must be able to provide services continuously, and for which interruptions (e.g., due to failures) are unacceptable or could be extremely damaging.

Release 15, SA6 has been working on the specification of functions to support the use of 3GPP networks by applications outside the 3GPP domain to enable the aforementioned cooperation with industrial applications. For example, SA6 specified the Common API Framework (CAPIF)[*5], a unified framework for northbound APIs[*6] provided by 3GPP, in Release 15, and introduced Service Enabler Architecture Layer for Verticals (SEAL)[*7], a set of functions that can be commonly used by various industrial applications, in Release 16.

This article presents an overview of the activities of SA6 and, in particular, describes two service frameworks, CAPIF and SEAL, which form a basis for coordinating industrial applications.

## 2. 3GPP SA6 Activities

Under the top-level Project Coordination Group (PCG)[*8], 3GPP has three Technical Specification Groups (TSGs)[*9]: Radio Access Network (RAN)[*10], which examines radio-related technologies; Service and System Aspects (SA)[*11], which examines service functions and overall system architecture; and Core Network and Terminals (CT)[*12], which examines core networks[*13], terminal interfaces and functions. Each TSG is subdivided into four to six working groups. SA6 was established in 2014 as a working group within TSG SA that examines functionality and architecture, especially for mission-critical applications.

When SA6 was first launched, SA6 worked on developing specifications for mission-critical services (push-to-talk[*14], video and data communications) with a focus on their use in the public safety[*15] field. Later, in Release 15, the release in which the initial 5G specifications were also formulated, CAPIF was formulated as a unified framework for northbound APIs provided by 3GPP. In Release 16 and later, SA6 has developed more frameworks that can be applied to various services in addition to mission-critical services and has studied enablement of applications in various industrial fields such as Vehicle-to-Everything (V2X)[*16], drones[*17] and smart factories[*18]. Currently, the scope of SA6's work is labeled as "application enablement and critical communication applications" [1]. SA6 specifies architecture for applications that utilize the 3GPP network.

## 3. CAPIF

### 3.1 Purpose of CAPIF Implementation

CAPIF was introduced in Release 15 to provide a unified framework for the various APIs provided by 3GPP. In 3GPP, service APIs are provided by the aforementioned SCEF, NEF and functional parts for Multimedia Broadcast/Multicast Service (MBMS)[*19]. On the other hand, when developing and using these APIs, there are common issues to be considered, such as publishing and managing exposed APIs and security-related functions. CAPIF serves as a framework for solving these common issues.

### 3.2 Architecture of CAPIF

Typical CAPIF architecture is shown in **Figure 1**.

[*5] CAPIF: A 3GPP framework that provides common functions for exposing northbound APIs.

[*6] Northbound API: An API that is provided to a higher-level application from the perspective of the device that provides the API.

[*7] SEAL: A layer of functions commonly used by multiple industrial applications using the 3GPP network.

[*8] PCG: The highest decision-making body of 3GPP, responsible for overall planning and progress management of 3GPP activities.

[*9] TSG: A group in 3GPP responsible for the development of technical specifications.

[*10] RAN: In 3GPP, a group that is working on specifications for networks consisting of base stations, etc. that control the radio layer and are located between the core network (see *13) and the User Equipment (UE).

[*11] SA: The 3GPP group handling specifications for service requirements, architectures, security, codecs and network administration.

[*12] CT: In 3GPP, the group responsible for specifications for protocols within the core network (see *13) and between UE and the core network.

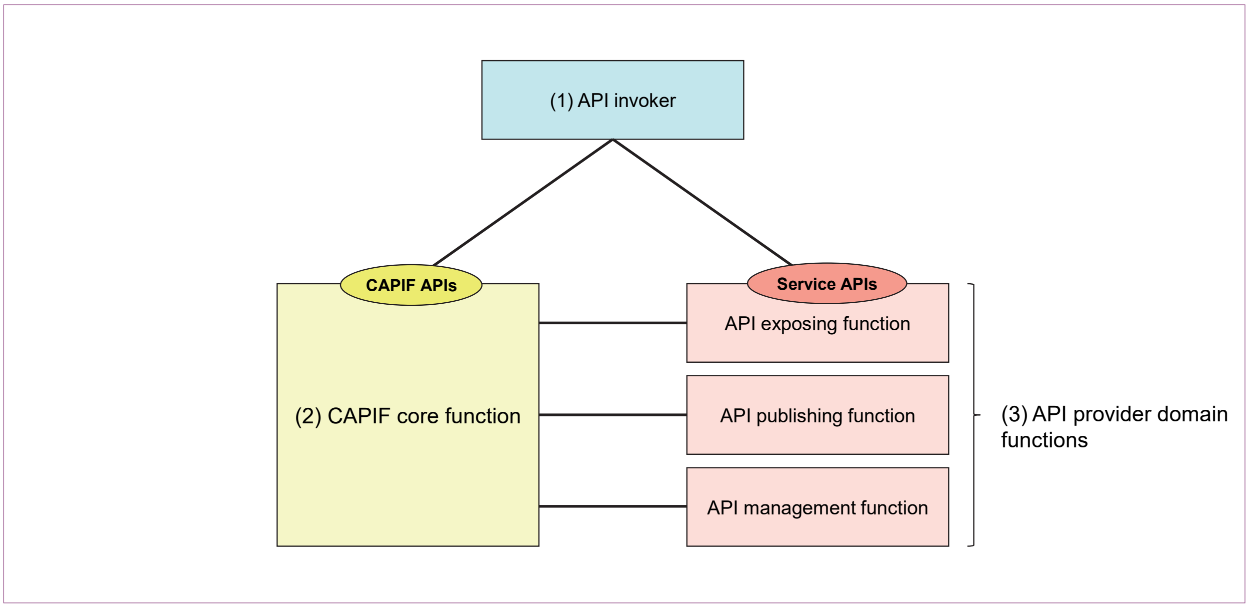

Figure 1　CAPIF architecture

1)　API Invoker

API invoker invokes the CAPIF APIs and service APIs. Both applications owned by network operators and applications owned by 3rd party providers other than network operators can be API invokers.

2)　CAPIF Core Function

CAPIF core function plays a central role in the various functions provided by CAPIF, such as API invoker authentication/authorization, API registration and policy management. These functions are provided as APIs, and each functional entity, including the API invoker, can use functions by invoking these APIs. The CAPIF core function is located in a domain that the mobile network operator can trust.

3)　API Provider Domain Functions

The three functional entities, *API exposing function, API publishing function* and *API management function*, are collectively called API provider domain functions. CAPIF defines the provider of CAPIF core functions as the CAPIF provider and the provider of API provider domain functions as the API provider, which can be two separate entities or the same entity.

The API exposing function is a functional entity that receives service API invocations from API invokers. The API publishing function is responsible for publishing service API information to the CAPIF core function to make service APIs available to API invokers. Finally, the API management function is responsible for the management of published service APIs and has functions such

[*13] Core network: A network comprised of switching equipment, subscriber information management equipment, etc. UE communicates with the core network via a radio access network.

[*14] Push-to-talk: A method of voice communications in which a call can be made only while a button is pressed, as in a transceiver.

[*15] Public Safety: Services for public safety, such as police, fire and emergency services.

[*16] V2X: A technology that enables communication between a vehicle and its surrounding environment, such as between the vehicle and other vehicles or between the vehicle and objects on the road (such as a traffic light).

[*17] Drone: An aircraft that is not piloted by a person on board. In 3GPP, systems that include drone-related functions are called Uncrewed Aerial System (UAS).

[*18] Smart Factory: A factory system that utilizes IoT and other communication technologies. In 3GPP, it is specifically called Factories of the Future (FF).

[*19] MBMS: A one-to-many (broadcast/multicast) communication service provided by the 3GPP system.

as auditing the service API invocation log and monitoring the service API status.

## 3.3 Functions of CAPIF

This section focuses on the three typical functions of CAPIF: API invoker onboarding, service API discovery and API invoker authentication and authorization. These functions are important as preliminary steps for API invokers to use a service API. For other detailed functions, please refer to [2].

1) API Invoker Onboarding

An API invoker must provide its own information to the CAPIF core function for approval prior to requesting a service API invocation. This procedure is called *onboarding*. If onboarding is successful, the API invoker will receive the information necessary for subsequent authentication and authorization.

Onboarding allows the CAPIF core function to recognize the API invoker and to authenticate and authorize the API invoker using the information obtained in this procedure. The CAPIF core function can also send information about the service APIs exposed to the API invoker.

2) Service API Discovery

For information on the service APIs that the API invoker can invoke, the API invoker can not only wait for the CAPIF core function to provide it in the onboarding procedure described above, but can also query the CAPIF core function. The procedure for obtaining service API information through this query is called service API discovery.

When an API invoker sends its identity information and the criteria for the API it wants to discover to the CAPIF core function, the CAPIF core function retrieves APIs that match the criteria from the stored API information. The CAPIF core function can also further filter the retrieved API information according to its own discovery policy. For example, it can exclude certain API categories from discovery. Sending the list of service APIs obtained in this way to the API invoker enables it to get information on target service APIs.

3) API Invoker Authentication and Authorization

An API invoker that has obtained information on a desired service API needs to go through the authentication and authorization process to invoke the service API. Authentication and authorization methods (hereinafter referred to as "security methods") used between the API invoker and the API exposing function are decided in advance between the API invoker and the CAPIF core function, based on information such as which security methods are supported by both. Three types of security methods are specified: *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS-PSK)*[*20], *Public Key Infrastructure (PKI)*[*21] and *TLS with OAuth*[*22] *token* [3]. The 3GPP TSG SA WG3 (SA3) is responsible for developing these detailed security-related specifications.

After determining the security method to be used, the API invoker requests authentication and authorization from the API exposing function prior to or upon the service API invocation. The API exposing function authenticates and authorizes the

[*20] TLS-PSK: A method of establishing a TLS connection that uses a Pre-Shared Key (PSK) to encrypt communications.

[*21] PKI: A mechanism for certifying the registrant of a public key used in cryptography. In this article, it refers specifically to the method of establishing a TLS connection using PKI.

[*22] OAuth: A standard specification for authorization of access privileges. In this article, it specifically refers to OAuth 2.0 specified in Internet Engineering Task Force Request for Comments (IETF RFC) 6749. Access privileges are controlled by issuing data called tokens.

API invoker based on a predetermined security method while cooperating with the CAPIF core function as necessary. An important role of CAPIF is to provide these security mechanisms in a unified manner.

## 4. SEAL

### 4.1 Purpose of SEAL Implementation

SEAL is a layer that brings together functions commonly used by multiple industrial applications that use 3GPP networks. In 3GPP, a vertical domain, or simply a vertical, is a set of industries and companies that provide services and products in a particular field, such as V2X, drones and smart factories. Each vertical application implements necessary functions according to its own requirements, although some functions are commonly required among multiple vertical applications. Providing such functions together as SEAL eliminates the need to implement them separately for each vertical application and leads to efficient system development.

### 4.2 Architecture of SEAL

Typical SEAL architecture is shown in **Figure 2**.

SEAL consists of a SEAL client, which performs client-side functions, and a SEAL server, which performs server-side functions. Both of them communicate with each other to realize functions such as location information management and group management. The SEAL server can make use of the functions provided by the 3GPP network system (e.g., APIs provided by NEF). When focusing on a particular SEAL function, a SEAL client or

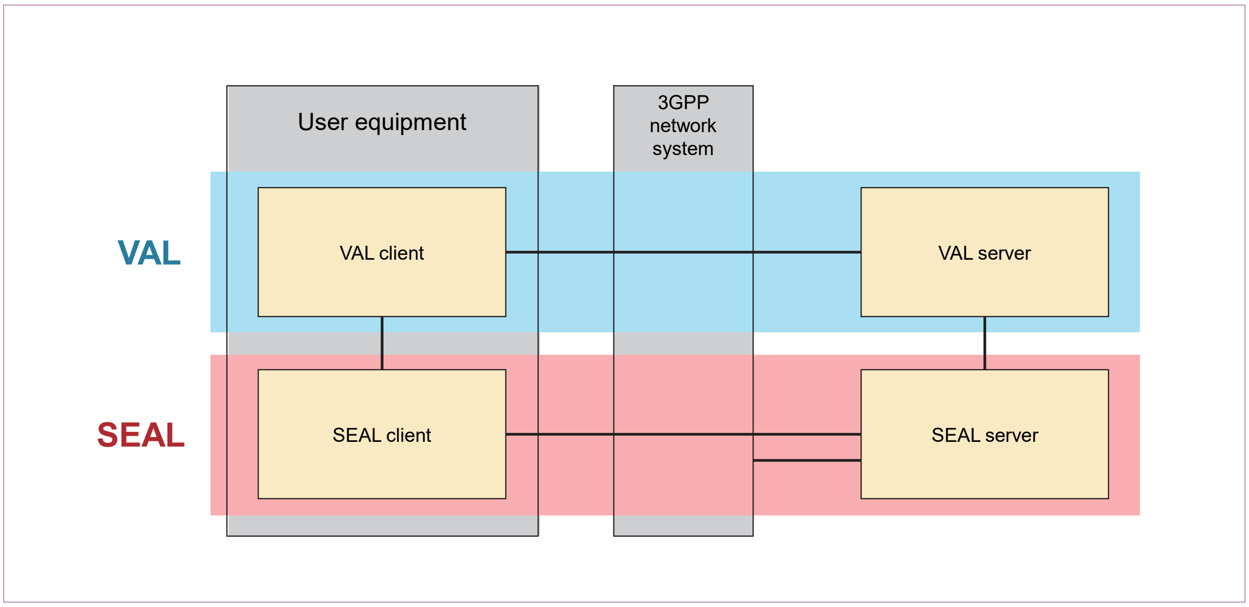

Figure 2 SEAL architecture

server may be referred to by the name of its function (e.g., a SEAL server for location management is specifically referred to as a location management server).

The Vertical Application Layer (VAL) is positioned above SEAL. VAL is the layer on which applications specific to each vertical (e.g., V2X applications) reside. VAL clients and VAL servers can use the functions provided by SEAL by communicating with SEAL clients and SEAL servers in the lower layer.

## 4.3 Functions of SEAL

This section focuses on three typical SEAL functions: location information management, group management and network resource management. SA6 is also studying individual solutions for each vertical and the use of the above three functions is being discussed in particular as part of these studies. For other detailed functions, please refer to [4].

1) Location Management

The SEAL client or server responsible for location management is called the location management client or server, respectively. The location management client and server can obtain information about the location of VAL service users.

For example, when the VAL server wants to obtain the location information of a specific VAL user, the VAL server sends a location reporting trigger to the location management server as a signal to start the location reporting procedure. After the location management server receives this signal, it queries the location management client for location information and sends the received location information to the VAL server.

It is possible to identify the location of other User Equipment (UE) from UE as well as from the VAL server. For example, to find out the location of UE on which location management client A is implemented, location management client B, which is implemented on different UE, can send a location reporting trigger to the location management server. As in the previous example, the location management server that receives the location reporting trigger queries location management client A for location information and sends the received location information to location management client B. This process enables the location management client to obtain the location information of the target device.

The time when location information is obtained can also be changed depending on the purpose. Specifically, when a VAL server or a location management client obtains location information of a specific VAL user, it can receive the location information immediately after sending a location information report trigger, or it can set specific conditions and receive the location information when the conditions are satisfied (e.g., the VAL server or the location management client receives the location information at regular intervals). In addition to receiving location information directly from the location management client, the location management server can also receive UE location information from the 3GPP network and send that information to the VAL server or other devices.

2) Group Management

The SEAL client and server responsible for group management are called group management client and server, respectively. The group management function allows the creation of a group consisting and multiple VAL users and management of members within that group.

For example, when a VAL user authorized to create groups wants to create a new group, the group management client of the VAL user sends a group creation request to the group management server. At this time, the identities of users to be included in the same group are also sent. Based on this request, the group management server creates a new group. After creating a group, a group management client can send a group information query request to the group management server to obtain information about the created group. The group management client can also add or delete group members by sending a group membership update request to the group management server.

It is also possible to create location-based groups when the group management service is used in combination with the location management service described above. In such a case, the group management server requests and obtains a list of users existing in a specific location from the location management server and creates a group with the users in the list. As shown in this example, multiple SEAL entities can be used to provide services.

3) Network Resource Management

The SEAL client or server responsible for network resource management is called the network resource management client or server, respectively. An example of network resource management service is to apply Quality of Service (QoS)*23 according to VAL services' requests.

To apply the desired QoS, the VAL server sends a network resource adaptation request to the network resource management server for specific UE (or UE group). Based on this request, the network resource management server allocates network resources to the target UE or UE group. The network resource management server also connects to 3GPP systems such as Policy Control Function (PCF)*24 and initiates Policy and Charging Control (PCC) procedures*25 based on requests. This makes it possible to apply QoS according to the requirements of each VAL service.

## 5. Conclusion

This article provided an overview of the activities of 3GPP SA6 and described the two frameworks, CAPIF and SEAL, which were standardized by SA6. These frameworks are expected to play a role in enabling industrial applications to utilize 3GPP systems. SA6 has been continuously enhancing CAPIF and SEAL since they were introduced in Release 15 and 16, respectively. NTT DOCOMO is contributing to the study of such enhancements. In Release 17 and later, the architecture for realizing edge computing*26 and technical specifications specific to services for individual industries such as V2X, drones and smart factories are also being discussed. SA6 has started technical studies for

*23 QoS: Quality of a communications service. Bandwidth and latency are typical indicators.

*24 PCF: A function of the 5G core network responsible for policy control such as QoS and billing control.

*25 PCC procedure: A series of processes related to policy control and billing control. Requests from the network resource management server are also reflected in the 3GPP system by the PCC procedure.

*26 Edge computing: A form of service in which computational processing is performed close to the UE. It is expected to reduce latency and to distribute network load.

Release 18. NTT DOCOMO will promote standardization activities in 3GPP SA6 with a view to further industrial application use cases.

## REFERENCES

[1] 3GPP SP-210265: "Terms of Reference (ToR) for 3GPP TSG SA WG6 (SA6)," Mar. 2021.

[2] 3GPP TS 23.222 V17.5.0: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2," Jun. 2021.

[3] 3GPP TS 33.122 V16.3.0: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs," Jul. 2020.

[4] 3GPP TS 23.434 V17.3.0: "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows," Sep. 2021.