3GPP TR 23.745 V17.0.0 (2021-09)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on application layer support for Factories of the Future in 5G network; (Release 17)

Keywords
<keyword[, keyword]>

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document is a technical report which identifies the application architecture aspects to support Factories of the Future in 5G network, and corresponding architectural solutions. The study includes identifying architecture requirements that are necessary to ensure efficient use and deployment of application layer support for Factories of the Future in 5G network.

The study takes into consideration the existing work including stage 1 requirements in 3GPP TS 22.261 [2] and 3GPP TS 22.104 [3], and provides recommendation for normative work.

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 22.261: "Service requirements for the 5G system; Stage 1".

[3] 3GPP TS 22.104: "Service requirements for cyber-physical control applications in vertical domains; Stage 1".

[4] IEEE 802.1Qbv-2015: "Standard for Local and Metropolitan Area Networks-Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks Amendment: Enhancements for Scheduled Traffic".

[5] IEEE 802.1AS-2011: "IEEE Standard for Local and Metropolitan Area Networks - Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks".

[6] IEEE 802.1Q-2018: "IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks".

[7] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[8] 3GPP TS 23.434: "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows;"

[9] oneM2M TS-0001: "Functional Architecture".

[10] 3GPP TS 23.558: "Architecture for enabling Edge Applications (EA)".

[11] 3GPP TS 29.522: "5G System; Network Exposure Function Northbound APIs; Stage 3".

[12] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

[13] 3GPP TR 23.700-20: "Study on enhanced support of Industrial Internet of Things (IIoT) in the 5G System (5GS)".

[14] 3GPP TS 29.549: "Service Enabler Architecture Layer (SEAL); Application Programming Interface (API) specification; Stage 3".

[15] 3GPP TS 23.503 : "Policy and charging control framework for the 5G System (5GS); Stage 2".

[16] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs".

[17] 3GPP TS 28.541: "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3".

[18] 3GPP TS 28.533: "Management and orchestration; Architecture framework".

[19] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[20] OPC 10000-1: "OPC Unified Architecture Specification Part 1: Overview and Concepts".

[21] OPC 10000-6: "OPC Unified Architecture - Part 6: Mappings".

[22] OPC 10000-14: "OPC Unified Architecture - Part 14: PubSub ".

[23] DIN SPEC 91345:2016-04: " Reference Architecture Model Industry 4.0 (RAMI4.0)".

[24] 3GPP TS 22.263: "Service requirements for video, imaging and audio for professional applications (VIAPA); Stage 1".

[25] IEEE Std 802.1Qcc-2018: "Standard for Local and metropolitan area networks - Bridges and Bridged Networks - Amendment: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements".

[26] 3GPP TS 29.122: "T8 reference point for Northbound APIs".

[27] IETF RFC 7252: "The Constrained Application Protocol (CoAP)".

[28] IETF RFC 8323: "CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets".

[29] IETF RFC 7959: "Block-Wise Transfers in the Constrained Application Protocol (CoAP)".

[30] IETF RFC 7641: "Observing Resources in the Constrained Application Protocol (CoAP)".

[31] IETF RFC 6690: "Constrained RESTful Environments (CoRE) Link Format".

[32] IETF RFC 8613: "Object Security for Constrained RESTful Environments (OSCORE)".

[33] IETF draft-ietf-ace-oauth-authz-35: "Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)".

[34] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[35] 3GPP TS 23.003: "Numbering, addressing and identification".

[36] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[37] IEEE Std 802.1CB-2017: "Frame Replication and Elimination for Reliability".

[38] 3GPP TS 22.262: "Message service within the 5G System (5GS); Stage 1".

[39] 3GPP TR 23.700-24: "Study on support of the 5GMSG (Message Service for MIoT over 5G System) Service".

[40] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.261 [2] apply:

5G LAN-type service

non-public network

private communication

private slice

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.104 [3] apply:

vertical domain

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5GC	5G Core Network
5GS	5G System
5GLAN	5G Local Area Network
5G LAN-VN	5G Local Area Network- Virtual Network
AS	Application Server
AF	Application Function
CAPIF	Common API Framework for 3GPP northbound APIs
CNC	Centralized Network Configuration
CUC	Centralized User Configuration
CoAP	Constrained Application Protocol
CSIF	Communication Service Interface
DS-TT	Device-side TSN translator
eMBB	enhanced Mobile Broadband
FAE	FF Application Enabler
FF	Factories of the Future
GST	Generic Slice Template
mMTC	massive Machine Type Communication
MIoT	massive Internet of Things
NEF	Network Exposure Function
NW-TT	Network-side TSN translator
OT	Operation Technology
PCF	Policy Control Function
PDU	Protocol Data Unit
S-NSSAI	Single Network Slice Selection Assistance Information
SCEF	Service Capability Exposure Function
SEAL	Service Enabler Architecture Layer for Verticals
TSC	Time Sensitive Communication
TSN	Time Sensitive Networking
UE	User Equipment
URLLC	Ultra Reliable Low Latency Communication
VAL	Vertical Application Layer

4 Analysis of existing standards

4.1 Analysis of TS 22.261

4.1.1 Description

3GPP TS 22.261 [2] describes the service and operational requirements for a 5G system which include detail 5G communication for automation requirements in factories of the future domain.

The following 5G system capabilities impact on application layer support for Factories of the Future are addressed:

- Network slicing;
- Network capability exposure;
- Non-public networks;
- 5G LAN-type service;
- Positioning services;
- Energy efficiency;
- Messaging aspects.

4.1.2 Analysis

Table 4.1.2-1 lists the potential requirements which may be applicable for application layer support for Factories of the Future in 5G network.

Table 4.1.2-1: Service requirements applicable for application layer

5G system capabilities	Reference	Factories of the future related service requirement description
Network slicing	Subclause 6.1.2 of 3GPP TS 22.261 [2]	Network slicing services requirements for slice selection, UE access to services from more than one network slice simultaneously, slice access constraints, cross-network slice coordination
Network capability exposure	Subclause 6.10.2 of 3GPP TS 22.261 [2]	API requirements for geographic location, monitor network resource, communication services, monitor UE status, private slice network status, manage non-public network & private slice(s), private slice infrastructure, automatic configuration services to non-public networks
Non-public networks	Subclause 6.25.2 of 3GPP TS 22.261 [2]	Non-public network services requirements for service continuity, network selection
5G LAN-type service	Subclause 6.26.2 of 3GPP TS 22.261 [2]	5G LAN-type service requirements for service continuity, 5G LAN-VN management, industrial setting, service exposure
Positioning services	Subclause 6.27.2 of 3GPP TS 22.261 [2]	Positioning service requirements for position-related data available, traceability to application, UE provide position-related data, dynamically update rate of the position-related data, negotiate positioning methods
Energy efficiency	Subclause 6.15.2 of 3GPP TS 22.261 [2]	Energy efficiency requirements for battery driven, constrained UEs. Some field devices in the production and processing plants are constrained (for instance battery-driven field devices). E.g. industrial sensors can use a wide variety of batteries depending on the use case,

		but in general they are highly constrained in terms of battery size.
Messaging aspects	Subclause 6.29.2 of 3GPP TS 22.261 [2]	MSGin5G Service requirements described in TS 22.262 to provide one to one, group and broadcast message services for thing-to-thing and person-to-thing communication with low end-to-end latency and high reliability of message delivery, in a resource efficient manner to optimize the resource usage in the network, and power saving in the user devices.

4.2 Analysis of TS 22.104

4.2.1 Description

Two aspects were addressed in 3GPP TS 22.104 [3] include:

- End-to-end service performance requirements and network performance requirements related to these end-to-end service performance requirements;
- Support for LAN-type services specific to industrial/high performance use cases. Related Ethernet functionalities include, for example, those in IEEE 802.1Qbv [4].

The following 5G system capabilities may have an impact on application layer support for Factories of the Future in 3GPP TS 22.104 [3] are captured:

- Clock synchronisation requirements;
- High accuracy positioning requirements;
- TSN enhancements;
- Energy efficiency.

4.2.2 Analysis

Table 4.2.2-1 lists the requirements which may be applicable to the application layer support for Factories of the Future in 5G network.

Table 4.2.2-1: Service requirements of factories of the future domain

5G system capabilities	Reference	Factories of the Future related service requirement
Clock synchronisation	Subclause 5.6.1 of 3GPP TS 22.104 [3]	The 5G system shall support to synchronize a UE's time clock to a global clock or a working clock and support a mechanism to process and transmit related time synchronization protocols for 3rd party applications which use those protocols.
	Subclause 6.2 of 3GPP TS 22.104 [3]	For infrastructure dedicated to high performance Ethernet applications, the 3GPP system shall support clock synchronisation defined by IEEE 802.1AS [5] across 5G-based Ethernet links with PDU-session type Ethernet and other Ethernet transports such as wired and optical (Ethernet Passive Optical Network)
High accuracy positioning	Subclause 5.7 of 3GPP TS 22.104 [3]	Corresponding high positioning requirements for horizontal accuracy, availability, heading, latency and UE speed for typical scenarios
TSN enhancements	Subclause 6.2 of 3GPP	3GPP system shall support enhancements for time-sensitive networking as defined by IEEE 802.1Q [6] for 5G-based Ethernet

	TS 22.104 [3]	links with PDU sessions type Ethernet
Energy efficiency	Subclause 5.2 of 3GPP TS 22.104 [3]	Communication service performance requirements for industrial wireless sensors. Industrial sensors can use a wide variety of batteries depending on the use case, but in general they are highly constrained in terms of battery size.

5 Key issues

5.1 Key issue 1 - Use of network slicing for FFAPP

3GPP TS 22.104 [3] introduces potential use cases for 5G communication for automation in factories of the future domain which can be distinguished in different application areas.

The individual use cases are arranged according to their major performance requirements and can be classified according to the basic 5G service types eMBB, mMTC and URLLC.

3GPP TS 23.501[7] define S-NSSAI to identify a Network Slice, an S-NSSAI is comprised of a Slice/Service type (SST) and a Slice Differentiator (SD). The SSTs which are standardised as eMBB, URLLC and MIoT. The Factory of the Future use cases are classified with 5G Slice/Service type (SST) shown in Table 5.1-1.

Table 5.1-1: Factory of the Future use cases classified with 5G Slice/Service type (SST)

Use case	**Application area**	**Reference**	**Slice/Service type(SST)**
Motion control	Factory automation	Subclause A2.2.1 of 3GPP TS 22.104 [3]	URLLC
Control-to-control communication	Factory automation/ Logistics and warehousing	Subclause A2.2.2 of 3GPP TS 22.104 [3]	URLLC
Mobile robots	Factory automation/ Process automation/ Logistics and warehousing	Subclause A2.2.3 of 3GPP TS 22.104 [3]	URLLC
Wired to wireless link replacement	Factory automation	Subclause A2.2.4 of 3GPP TS 22.104 [3]	URLLC
Cooperative carrying	Factory automation	Subclause A2.2.5 of 3GPP TS 22.104 [3]	URLLC
Closed-loop process control	Process automation	Subclause A2.3.1 of 3GPP TS 22.104 [3]	URLLC
Process monitoring	Process automation	Subclause A2.3.2 of 3GPP TS 22.104 [3]	URLLC
Plant asset management	Process automation/ Logistics and warehousing	Subclause A2.3.3 of 3GPP TS 22.104 [3]	eMBB
Mobile control panels with safety	HMIs and production IT	Subclause A2.4.1 of 3GPP TS 22.104 [3]	URLLC
Augmented reality	HMIs and production IT	Subclause A2.4.2 of 3GPP TS 22.104 [3]	eMBB
Remote access and maintenance	Monitoring and maintenance	Subclause A2.5.1 of 3GPP TS 22.104 [3]	eMBB

3GPP TS 22.261 [2] describes the service and operational requirements for a 5G system which include detail 5G communication for automation requirements in factories of the future domain. Network slicing is one of the 5G system capabilities may impact on application layer support for Factories of the Future.

Open issues：

Are the slicing support functions specified by SA5 and SA2 sufficient for FFAPP requirements?

5.2 Key issue 2 - Geographic location and positioning information support

In 3GPP TS 22.104 [3], some Factories of the Future related typical scenarios and corresponding high accuracy positioning requirements (horizontal accuracy, availability, heading, latency and UE speed) were described. Scenario such as augmented reality in smart factories, inbound logistics for manufacturing require ms level latency for position estimation of UE.

In 3GPP TS 22.261 [2], positioning service requirements were defined for 5G system to support those postioning related vertical domian applications (including Factories of the Future). So far, there are several positioning methods supported by 5G system with different quality level.

A suitable API was also designed in 5G system to be exposed to an authorised 3rd party to provide the information regarding the availability status of a geographic location that is associated with that 3rd party.

Open issues:

1) Study is needed to evaluate existing 5G positioning solutions to meet the positioning requirements of Factories of the Future applications.

2) How to support positioning method with ms-level latency requires further study?

3) What positioning methods are needed to supply absolute and relative positioning for different 5G positioning services requires further study.

4) Whether and how SEAL's Location Management service can be utilized for FFAPP's location acquisition and location reporting scenarios and also if any enhancement is required for SEAL's Location Management service to support the same.

5.3 Key issue 3 - Clock synchronization

In 3GPP TS 22.104 [3], it is required that 5G system shall support a mechanism to process and transmit related protocols and support to synchronize a UE's time clock to a global clock or a working clock. Furthermore, 5G system shall support clock synchronisation defined by IEEE 802.1AS [5] across 5G-based Ethernet links with PDU-session type Ethernet or other Ethernet transports such as wired and optical (Ethernet Passive Optical Network). So far, several options were proposed in 5G system for clock synchronization.

Clock synchronization is needed e.g. for Time Sensitive Communication services in TSN and non-TSN scenarios. Exposure of 5GS time synchronization capabilities, e.g. 5GS support for time synchronization, time synchronization methods and other parameters, can be learned and used by FF UEs and applications.

Open issue:

a. Further study is required to determine whether and how to manage and utilize 5G clock synchronization mechanism according to subclause 5.6.1 and 6.2 of 3GPP TS 22.104 [3].

b. Investigate whether and how SEAL should support exposure of clock synchronization capabilities.

5.4 Key issue 4 - TSN supporting

Time-Sensitive Networking (TSN) is an important functionality of industrial communication networks. Such industrial communication networks are usually IEEE 802.1-based networks with Ethernet links (non-3GPP network).

5G networks provide advantages for cyber-physical control applications with respect to flexibility and mobility due to their radio access network with low latency, high availability, high reliability, and time synchronization capabilities over wireless links. On the other hand, IEEE-802.1-based TSN networks provide advantages with wired connectivity for cyber-physical control applications, especially for demanding real-time control applications and periodic-deterministic communication, also with very high availability requirements.

Due to the different pros and cons, many industrial communication networks will deploy both, non-public 5G networks and IEEE 802.1-based TSN networks. An integration of 5G networks and IEEE 802.1-based TSN networks is necessary. The proper integration of 5G networks and TSN networks can also require the acquisition of service requirements that may not be yet in the scope of the current 5G QoS framework. One such parameter is the survival time as specified in 3GPP TS 22.104 [3] which reflects an application's resilience to consecutive transmission failures of the application data. The survival time which is seen as an application QoS attribute (i.e. service performance requirement, as specified in TS 22.104 [3]), should be taken into account when the TSN system provides/adapts the service requirements to the 5GC or the UE, since this may have impact on the network QoS configuration.

3GPP TS 23.501 [7] describes 5G System features that support Time Sensitive Communications (TSC) and allow the 5G System to be integrated transparently as a bridge in an IEEE TSN network. Periodic deterministic QoS feature allows the 5GS to support periodic deterministic communication where the traffic characteristics are known a-priori, and a schedule for transmission from the UE to a downstream node, or from the UPF to an upstream node is provided via external protocols outside the scope of 3GPP (e.g. IEEE TSN).

The features include the following:

- Providing TSC Assistance Information (TSCAI) that describe TSC flow traffic patterns at the 5GS egress interfaces
- Support for hold & forward buffering mechanism in the TSN Translator on the UE side and UPF side to de-jitter flows that have traversed the 5G System.

For support of integration with TSN, in order to schedule TSN traffic over 5GS Bridge, the configuration information of 5GS Bridge is mapped to 5GS QoS within the corresponding PDU Session.

TSN QoS monitoring functionality is described as follows:

1) In control plane, TSN QoS monitoring may interact with TSN AF, NEF and PCF.

2) In data plane, FAE client in the UE may get information from DS-TT directly.

Open issues：

How to monitor QoS parameters for 5GS Bridge configuration supported by 5GC, from the application layer of Factories of the Future to assure E2E QoS needs further study?

How to enable the translation of TSN application QoS requirements (e.g. survival time) to network QoS parameters, and what would be the impact on 5GS for QoS enforcement?

5.5 Key issue 5 - QoS monitoring

3GPP TS 22.261 [2] describes the QoS monitoring requirements specified for particular services such as URLLC services, vertical automation communication services which should be supported by 5G system. The following requirements:

The 5G network shall provide an interface to application for QoS monitoring (e.g. to initiate QoS monitoring, request QoS parameters, events, logging information, etc.).

The 5G system shall be able to provide real time QoS parameters and events information to an authorised application.

Open issues：

Whether and how to support the QoS monitoring from the application layer of Factories of the Future based on the 5GC QoS monitoring capabilities?

How to have common QoS monitoring solution for all verticals in SEAL?

5.6 Key issue 6 - 5GLAN group management

3GPP TS 22.261 [2] describes 5G LAN-type service and 5GLAN traffic types, service exposure requirements as follow:

The 5G system shall support 5G LAN-type service in a shared RAN configuration.

The 5G system shall support 5G LAN-type service over a wide area mobile network.

The 5G network shall support service continuity for 5G LAN-type service, i.e., the private communication between UEs shall not be interrupted when one or more UEs of the private communication move within the same network that provides the 5G LAN-type service.

The 5G system shall support use of unlicensed as well as licensed spectrum for 5G LAN-type services.

The 5G system shall enable the network operator to provide the same 5G LAN-type service to any 5G UE, regardless of whether it is connected via public base stations, indoor small base stations connected via fixed access, or via relay UEs connected to either of these two types of base stations.

The 5G system shall support traffic scenarios typically found in an industrial setting (from sensors to remote control, large amount of UEs per group) for 5G LAN-type service.

The 5G network shall provide suitable APIs to allow a trusted 3rd party to add/remove an authorized UE to/from a specific 5G LAN-VN managed by the trusted 3rd party.

3GPP TS 23.501 [7] describes features to support 5G LAN Group Management. 5G System supports management of 5G VN Group identification and membership (i.e. definition of 5G VN group identifiers and membership) and 5G VN Group data (i.e. definition of 5G VN group data). In order to support dynamic management of 5G VN Group identification and membership, the NEF exposes a set of services to manage (e.g. add/delete/modify) 5G VN group and 5G VN member. The NEF also exposes services to dynamically manage 5G VN group data.

3GPP TS 22.104 [3] describes Ethernet applications:

"This clause lists the requirements applicable to the 5G system for supporting cyber-physical applications using Ethernet.

For requirements pertaining to common, fundamental Ethernet transport requirements, and any requirements necessary to support the 5G LAN-type service, see Clause 6.24 in TS 22.261 [2]."

The following Ethernet applications requirements:

For infrastructure dedicated to high performance Ethernet applications, the 3GPP system shall support enhancements for time-sensitive networking as defined by IEEE 802.1Q [6], e.g. time-aware scheduling with absolute cyclic time boundaries defined by IEEE 802.1Qbv [4], for 5G-based Ethernet links with PDU sessions type Ethernet.

The Ethernet transport service shall support routing based on information extracted from the Ethernet header information created based on 802.1Qbv [4].

Open issues for the application layer support of Factories of the Future：

a. How to integrate 5G LAN type service with TSN for group management?

b. Investigate whether and how SEAL Group management service should support 5GLAN group management.

5.7 Key Issue 7 - Device Onboarding

Device onboarding is the process by which new devices are connected to the network for the first time and by which they gain at least the baseline connectivity and networking services so that they and the applications they run can boostrap themselves with further network or application layer procedures.

When done on scale, for instance in a factory environment with a huge number of different types of devices present, device onboarding needs to be as automatic as possible. On the other hand, it needs to be secure, authorized and follow the policies of both the network provider and the organization deploying the devices.

The overall process of onboarding devices can include the use of tools such as device management, credentials and subscription management, and network connectivity management. For many of these solutions and technologies exist.

Open issues:

a. Investigate mechanisms that can improve the overall process of device onboarding for factories of the future in the scope of SA6 work.

b. Investigate the usage of existing device onboarding technologies, e.g. oneM2M, GSMA, etc.

c. Investigate whether and how SEAL's Identity management service and Configuration management service can be utilized for device onboarding and authorization. Also investigate if any enhancements (e.g. considering the issue described in bullet a) are required in SEAL's Identity management service and Configuration management service to address this scenario.

NOTE: If an existing solution is identified to meet the requirements for this KI, the usage of that technology will be considered for inclusion in the TR

5.8 Key issue 8 - Communication of FF application requirements with 5GS

3GPP TS 22.104 [3] describes a communication service interface (CSIF) for supporting distributed automation applications. The CSIF is applicable for several factory automation applications including:

- Device to Device;
- Device to Controller and Controller to Device;
- Controller to Controller;
- Line Controller to Controller;
- Device to Cloud;

The 5G system has considered to support all these CSIF patterns and provides the transport (IP connectivity) to the FFAPP CSIF patterns. The CSIF patterns may utilize TSN.

The service requirements for different CSIF patterns vary in many aspects, e.g., packet size, packet transmission interval, reliability, packet loss rate, etc. And those requirements have to be mapped to 5G system QoS to guarantee the critical and deterministic communication.

Currently 5GS supports the QoS translation only for TSN networks as specified in TS 23.501 [7] (via CNC and TSN AF). FF applications can also be deployed in non-TSN for which the QoS translation is not supported.

Hence, it is required to study the application layer capability to analyze and communicate the service requirements for different FF applications' CSIF patterns to the 5G system.

5.9 Key issue 9 - Communication service on the Edge deployments

According to the TS 22.104 [3] clause 5.1, a local approach for the communication service on the network side is preferred to reduce the latency (between UE to UE via Uu and UE to network server) or to keep sensitive data in a non-public network on the factory site.

Open issues：

- How to support FFAPP communications over Edge deployments on network side?
- How to support/enable privacy for FFAPP sensitive data over Edge deployments?

5.10 Key issue 10 - Integration with Existing Operation Technologies

In factory floor applications, existing Operation Technologies are already deployed (e.g. OPC-UA). The 3GPP specified application layer services defined by SA6 will need to integrate with those existing technologies in order to be utilized in those deployments.

3GPP TS 22.104 [3] describes a communication service interface (CSIF) for supporting distributed automation applications. The CSIF is applicable for several factory automation applications including:

- Device to Device;
- Device to Controller and Controller to Device;
- Controller to Controller;
- Line Controller to Controller;
- Device to Cloud;

The 5G system has considered support for all of these CSIF patterns and provides the transport (IP connectivity) to these CSIF patterns. The CSIF patterns may utilize TSN for transport capabilities or integrate with existing OT systems at a higher layer. The existing Operation Technologies include the capability to meet these CSIF patterns.

It is required to study:

- The identification of relevant Operation Technologies;
- The ability to integrate to those identified Operation Technologies;
- The specifiction of the interaction of SA6-defined application layer capability with the identified Operation Technologies;

5.11 Key issue 11 - QoS coordination

The 5G system provides transport capabilities for different communication patterns between devices involved in FFAPP applications. Each FFAPP application may require different QoS considerations from the underlying 5G system.

The service requirements of FFAPP applications between different devices vary in many aspects, e.g., packet size, packet transmission interval, reliability, packet loss rate, etc. Those requirements are determined by the sending party or the receiveing party.

In current 5G QoS control model, the QoS parameters is preconfigured at PCF or negotiated between AF and PCF. While, for the device-to-device type of FFAPP application not based on TSN, there are no means to coordinate these service requirements to enable QoS on the communications between the devices.

Hence, it is required to study the QoS coordination method to support QoS based communications for one or more FFAPP applications between the devices when not using TSN.

5.12 Key Issue 12 - User authorization

User's consent is an important aspect while dealing with sensitive information about the user or the devices of the user. With the capabilities of the FF Application Servers to request invocation of 3GPP network capability exposure APIs,

such as location APIs, to obtain information about the user and the devices of the user, it is of utmost importance to capture the consent of the user.

Open issue:

- Whether and how to obtain user's consent to allow an FF Application specific server's service or information request?

Editor's Note: The solution for user consent is in the scope of SA3.

5.13 Key Issue 13: Capability Exposure related to Private Slice Network Status

The requirement of capability exposure is specified in subclause 6.10.2 of 3GPP TS 22.261 [2] and analysed in Table 4.1.2-1 in which private slice network status is required.

Issues include:

- Whether and how additional service APIs related to private slice network status are required to be supported at the factories of the future application enabler layer.

- Whether and how CAPIF can be leveraged for additional service APIs.

5.14 Key Issue 14 – Device monitoring

In Factories of the Future setting, the application require reliable and accurate operations from the onboarded devices. Hence, it is required that each device or group of devices are monitored and any change in its status is notified to the application layer (e.g. connectivity status, location change).

Further study is required to investigate whether the SEAL service(s) APIs specified in 3GPP TS 23.434 [4] towards the FF application specific layer are sufficient or additional events (e.g. establishment or change in connectivity, change in location, availability in group) from FAE layer/SEAL are required.

5.15 Key Issue 15 – Support for group communication

In Factories of the Future setting, large scale of devices are grouped and multicast/broadcast type group communication operations are required for application layer operations which can be enabled over different transport layer (e.g. PC5, Uu).

Currently, 3GPP TS 22.104 [3] has specified requirements for multicast/broadcast communications on group of UEs. To support FF application layer for group communication operations, it is required to investigate the following:

- Whether and how SEAL network resource management service specified in 3GPP TS 23.434 [8] can support FF application broadcast/multicast group communication operations.

- Whether and how SEAL group management service specified in 3GPP TS 23.434 [8] can support group management capabilities (e.g. create group, group join, group leave, group delete, group status notification) for FF application broadcast/multicast group communication operations.

The key issue involving group communication for 5G-LAN is addressed in clause 5.6.

5.16 Key Issue 16 – Constrained devices

Energy efficiency requirements are relevant for battery driven industrial devices. E.g. industrial wireless sensors can use a wide variety of batteries depending on the use case, but in general they are highly constrained in terms of battery size. It is important to analyse what impact the support for the use of constrained devices may have on the factories of the future architecture, e.g. whether a SIP- and HTTP-based architecture is suitable for such devices.

Open issues:

- Evaluate whether there are any impacts on the factories of the future architecture because of the use of constrained devices.
- Determine whether and how SEAL would need to be enhanced to address those impacts.

5.17 Key Issue 17 – Using 5G CN capabilities for SEAL Groups

Various key issues and solutions of this document, as listed below, illustrate leveraging SEAL services to fulfil the FF application layer requirements with assistance of core network.

Key Issues

- Key issue 6 - 5GLAN group management
- Key Issue 14 – Device monitoring
- Key Issue 15 – Support for group communication

Solutions

- Solution #1: FF application layer functional model
- Solution #7 Geographic location and positioning information support
- Solution #8: QoS monitoring
- Solution #9: 5GLAN group management
- Solution 15: Time Synchronization Management
- Solution #18: Device monitoring

These solution alternatives require SEAL server's interaction with 5GC via NEF as specified in TS 29.522 [11]. To invoke any NEF/SCEF APIs by the SEAL layer to fulfill the FF application layer requirements, the SEAL layer needs to identify the UE or a group of UEs, for which the NEF/SCEF APIs are to be invoked. SEAL layer can use external identifier of the UE (as specified in 3GPP TS 23.682 [34]) to invoke the NEF/SCEF APIs.

When supported by the SCEF/NEF, the key issues and solutions described above may be able to invoke the SCEF/NEF APIs. The SCEF/NEF APIs (like Monitoring API), support 'External Group Identifiers', as specified in TS 23.682 [34] (clause 4.6.3), to identify a group of UEs in the request. An External Group Identifier maps to an IMSI-Group Identifier(s) (defined in TS 23.003 [35]) that are stored in the HSS/UDM. Currently SEAL is not utilizing the 3GPP CN identification (external group ID) for group of UEs to invoke NEF/SCEF APIs.

Open issue:

- How SEAL uses external group identifier managed by 3GPP CN for VAL groups is FFS?
- Whether current mechanisms provided by 3GPP CN are sufficient to manage group of FFAPP UEs to enable SEAL to invoke 3GPP CN APIs for the group is FFS.

5.18 Key Issue 18 – Support for Message communication

The MSGin5G Service as specified in 3GPP TS 22.262 [38] has requirements related to one to one, group and broadcast message services for thing-to-thing and person-to-thing communication with low end-to-end latency and high reliability of message delivery, in a resource efficient manner. Further, 3GPP TR 23.700-24 [39] has defined solutions for these requirements. And 3GPP TS 22.261 [2] also describes similar message communication requirements that are applicable for FFAPP.

It is required to study following:

- Whether and how MSGin5G Service communication mechanisms specified in 3GPP TR 23.700-24 [39] can be leveraged for FFAPP message communication?

Editor's note: Considering other messaging mechanisms/services (e.g. OPC UA, CoAP) is FFS.

6 Architectural requirements

6.1 General requirements

6.1.1 Description

This subclause specifies the general requirements for FF application layer functional architecture.

6.1.2 Requirements

[AR-6.1.2-a] The FAE architecture shall support one or more FF applications.

[AR-6.1.2-b] The FAE capabilities shall be offered via APIs to the FF applications.

[AR-6.1.2-c] The FAE capabilities shall support obtaining information of the available FF services (e.g. identified by FF service ID) from the FF application to FF UEs.

[AR-6.1.2-d] The FAE client shall be able to communicate to multiple FAE servers.

6.2 Requirements for supporting time sensitive communication services

6.2.1 Description

This subclause specifies the requirements for FF application layer functional architecture with respect to TSC type of traffic.

6.2.2 Requirements

[AR-6.2.2-a] The FFAPP application layer functional architecture shall provide support for time sensitive communication services.

[AR-6.2.2-b] The FFAPP application layer functional architecture shall support control plane mechanisms related to TSN AF (as defined in TS 23.501 [7]).

[AR-6.2.2-c] The FFAPP application layer functional architecture shall support mechanisms, on top of TSN AF (as defined in TS 23.501 [7]), to adapt the TSN 5GS bridge as per application requirements.

7 Solutions

7.1 Solution #1: FF application layer functional model

7.1.1 Solution description

7.1.1.1 General

This solution provides the architecture and functional model required for addressing the application layer support aspects.

7.1.1.2 FF application layer functional model

Figure 7.1.1.2-1 illustrates the FF application layer functional model.

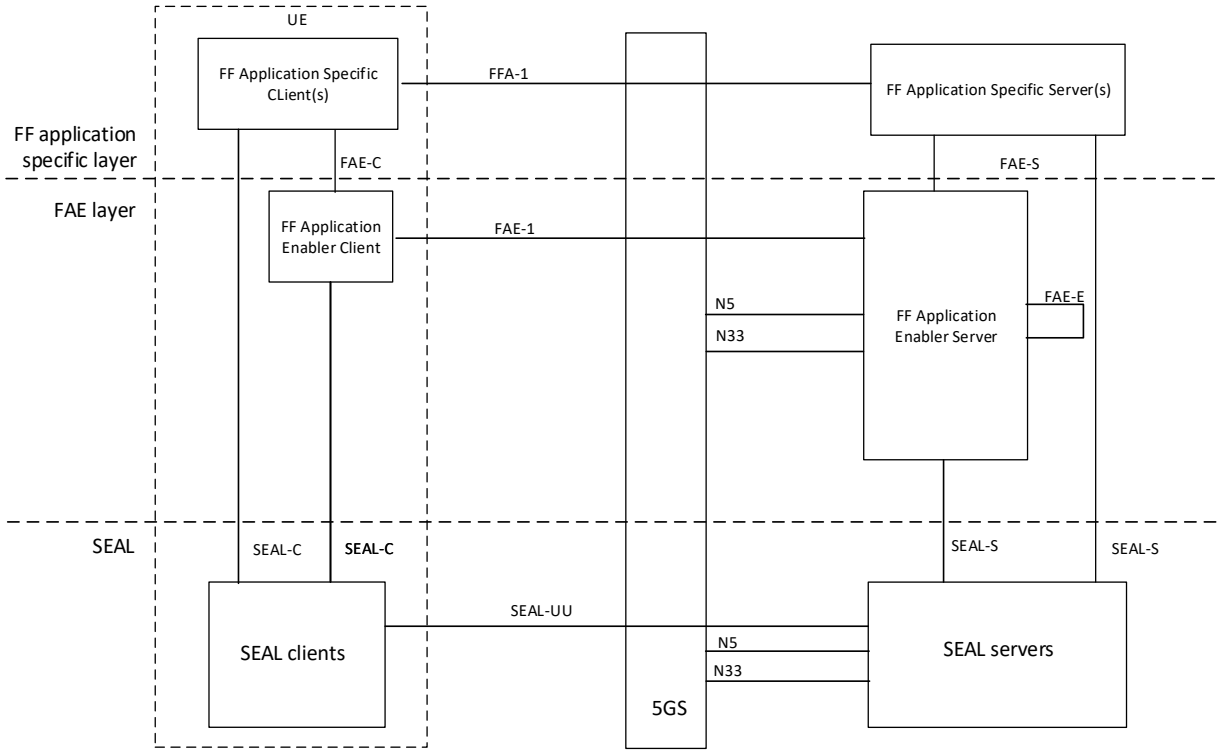

Figure 7.1.1.2-1: FF application layer functional model

Editor's note: How the FF Application server will be represented in the functional diagram will be considered in normative work

The FF application layer functional entities for the FF UE and the FF application server are grouped into the FF application specific layer and the FF Application Enabler (FAE) layer. The FAE layer offers the FAE capabilities to the FF application specific layer. The FF application specific layer consists of the FF application specific functionalities.

The FF Application Server (AS) consists of the FAE server and the FF application specific server(s). The FAE server provides the FF application layer support functions to the FF application specific server(s) via FAE-S reference point.

The FF UE consists of the FAE client and the FF application specific client(s). The FAE client provides the FF application layer support functions to the FF application specific client(s) via FAE-C reference point.

NOTE 1: The definition of FAE-C reference point is out of scope of the present document.

In the FAE layer, the FAE client communicates with the FAE server over FAE-1 reference point. In the FF application specific layer, the FF application specific client(s) communicates with FF application specific server(s) over FFA-1 reference point.

NOTE 2: The definition of FFA-1 reference point is out of scope of the present document.

The FAE server interacts with another FAE server over FAE-E reference point.

FAE server (acting as AF) interacts with the 3GPP system (5GS) over N5 reference point as specified in 3GPP TS 23.501 [7]. FAE server interacts with the 3GPP system (5GS) over N33 reference point as specified in 3GPP TS 23.501 [7]. When CAPIF is supported, the FAE server acts as the API Invoker and interacts with NEF acting as API provider domain functions and interacts with CAPIF Core Function, as specified in 3GPP TS 23.222 [16]. When CAPIF is supported, the FF application specific server acts as the API invoker and interacts with FAE server and SEAL

server(s) where both are acting as API provider domain functions and interacts with CAPIF Core Function, as specified in 3GPP TS 23.222 [16].

The FF application specific server(s) and FF application enabler server consume SEAL services over SEAL-S reference point. The FF application specific client(s) and FF application enabler client consume SEAL services over SEAL-C reference point.

The following SEAL services for FF applications are supported:

- Location management as specified in 3GPP TS 23.434 [8];
- Group management as specified in 3GPP TS 23.434 [8];
- Configuration management as specified in 3GPP TS 23.434 [8];
- Identity management as specified in 3GPP TS 23.434 [8];
- Key management as specified in 3GPP TS 23.434 [8]; and
- Network resource management as specified in 3GPP TS 23.434 [8].

SEAL can further be enhanced to use a new QoS monitoring capability in order to provide network resource monitoring functionality either as an enhancement of the Network Resource Management service or as a new Network Resource Monitoring service via N33. SEAL-S reference point will thus support QoS monitoring for URLLC services, e.g. TSC services.

SEAL Network Resource Management can further be enhanced to provide Time Synchronization Management capabilities in its service via N33. SEAL-S reference point will thus support Time Synchronization Management for URLLC services supported by 5GS, e.g. for TSC services.

The FAE client interacts with SEAL clients over the SEAL-C reference point specified for each SEAL service. The FAE server interacts with SEAL servers over the SEAL-S reference point specified for each SEAL service. The interaction between a SEAL client and the corresponding SEAL server is supported by SEAL-UU reference point specified for each SEAL service.

NOTE 3: The SEAL-C, SEAL-S, SEAL-UU reference points for each SEAL service is specified in 3GPP TS 23.434 [8].

7.1.1.3 Functional entities description

7.1.1.3.1 General

Each subclause is a description of a functional entity corresponding to FF application layer and does not imply a physical entity.

7.1.1.3.2 FF application specific client

The FF application specific client provides the client side functionalities corresponding to the FF applications (e.g. motion control, control-to-control communication, mobile robots, process automation – process monitoring, mobile control panels, remote access and maintenance). The FF application specific client(s) utilizes the FAE client for the FF application layer support functions.

NOTE 4: The details of the FF application specific client is out of scope of the present document.

7.1.1.3.3 FF application specific server

The FF application specific server provides the server side functionalities corresponding to the FF application(s) (e.g. motion control, control-to-control communication, mobile robots, process automation – process monitoring, mobile control panels, remote access and maintenance). The FF application specific server(s) utilizes the FAE server for the FF application layer support functions.

NOTE 5: The details of the FF application specific server is out of scope of the present document.

7.1.1.3.4 FAE client

The FAE client provides the UE side FF application layer support functions and supports interactions with the FF application specific client(s).

7.1.1.3.5 FAE server

The FAE server provides the server side FF application layer support functions and supports interactions with FF applications specific server(s).

The FAE server also support interactions with other FAE server(s).

7.1.1.3.6 SEAL client

The following SEAL client defined in 3GPP TS 23.434 [8] can be utilized by FF applications:

- Location management client;
- Group management client;
- Configuration management client;
- Identity management client;
- Key management client;
- Network resource management client.

7.1.1.3.7 SEAL server

The following SEAL server defined in 3GPP TS 23.434 [8] can be utilized by FF applications:

- Location management server;
- Group management server;
- Configuration management server;
- Identity management server;
- Key management server and;
- Network resource management server.

7.1.1.4 Reference points

7.1.1.4.1 General

The reference points for the FF application layer are described in the following subclauses.

7.1.1.4.2 FAE-1

The interactions related to FF application layer support functions between FAE client and FAE server are supported by FAE-1 reference point.

7.1.1.4.3 FFA-1

The interactions related to FF application layer support functions between FF application specific client and FF application specific server are supported by FFA-1 reference point. The details of FFA-1 reference point is out of scope of the present document.

7.1.1.4.4 FAE-E

The interactions related to FF application supports functions between the FAE servers are supported by FAE-E reference point.

7.1.1.4.5 FAE-S

The interactions related to FF application layer support functions between FF application specific server and FAE server are supported by FAE-S reference point.

7.1.1.4.6 FAE-C

The interactions related to FF application layer support functions between FF application specific client and FAE client are supported by FAE-C. The details of FAE-C reference point is out of scope of the present document.

7.1.1.4.7 SEAL-C

The following SEAL-C reference points for V2X applications can be re-used by FF application(s):

- LM-C reference point for location management as specified in 3GPP TS 23.434 [8];
- GM-C reference point for group management as specified in 3GPP TS 23.434 [8];
- CM-C reference point for configuration management as specified in 3GPP TS 23.434 [8];
- IM-C reference point for identity management as specified in 3GPP TS 23.434 [8];
- KM-C reference point for key management as specified in 3GPP TS 23.434 [8];
- NRM-C reference point for network resource management as specified in 3GPP TS 23.434 [8].

7.1.1.4.8 SEAL-S

The following SEAL-S reference points for V2X applications can be re-used by FF application(s):

- LM-S reference point for location management as specified in 3GPP TS 23.434 [8];
- GM-S reference point for group management as specified in 3GPP TS 23.434 [8];
- CM-S reference point for configuration management as specified in 3GPP TS 23.434 [8];
- IM-S reference point for identity management as specified in 3GPP TS 23.434 [8];
- KM-S reference point for key management as specified in 3GPP TS 23.434 [8];
- NRM-S reference point for network resource management as specified in 3GPP TS 23.434 [8].

7.1.1.5 External reference points

7.1.1.5.1 General

The reference points between the FF application layer and the 3GPP network system (5GS) are described in the following subclauses.

7.1.1.5.2 N5

The reference point N5 supports the interactions between the FF AS and the PCF is specified in 3GPP TS 23.501 [7]. The functions for N5 reference point are supported by FAE server.

7.1.1.5.3 N33

The reference point N33 supports the interactions between the NEF and FF AS is specified in 3GPP TS 23.501 [7]. The functions of N33 interface are supported by FAE server.

7.1.2 Solution evaluation

This solution provides a viable functional model for FF application architecture.

7.2 Solution #2: Establishing communication with FF application service requirements

7.2.1 Solution description

This solution corresponds to the key issue #8 on communication of FF application requirements with 5GS and key issue#11 on QoS coordination.

In this solution, a FAE client and FAE server (acting as an AS) are involved in the exchange and analysis of the desired service requirements (e.g. packet size, packet transmission interval, reliability, packet loss rate) for the communication amongst the FF application UEs when not using TSN. The FAE server triggers the establishment of direct service connectivity based on the information provided by the UEs and static configuration information available to the FAE server prior to the UE interaction. Note that service connectivity among FF application specific clients is established over the FFA-2 reference point, without device-to-device direct radio connectivity (e.g. PC 5) requirement.

The procedure for establishing FFA-2 service communication with FF application service requirements is as illustrated in figure 7.2.1-1.

Pre-condition:

- FAE client 1 and FAE client 2 are provided configuration information for the FF application specific clients served e.g. connectivity requirements, which destination UEs to connect to over FFA-2, etc.
- The FAE client 1 and FAE client 2 are configured with the information of the FAE server and have connectivity enabled to communicate with the FAE server. The information is provided via pre-configuration.
- The FAE server is configured with policies and information of the UEs to determine authorization of the UEs requesting connectivity via FFA-2.
- The FF application specific clients associated with FAE client 1 and FAE client 2 have triggered the establishment of connectivity.

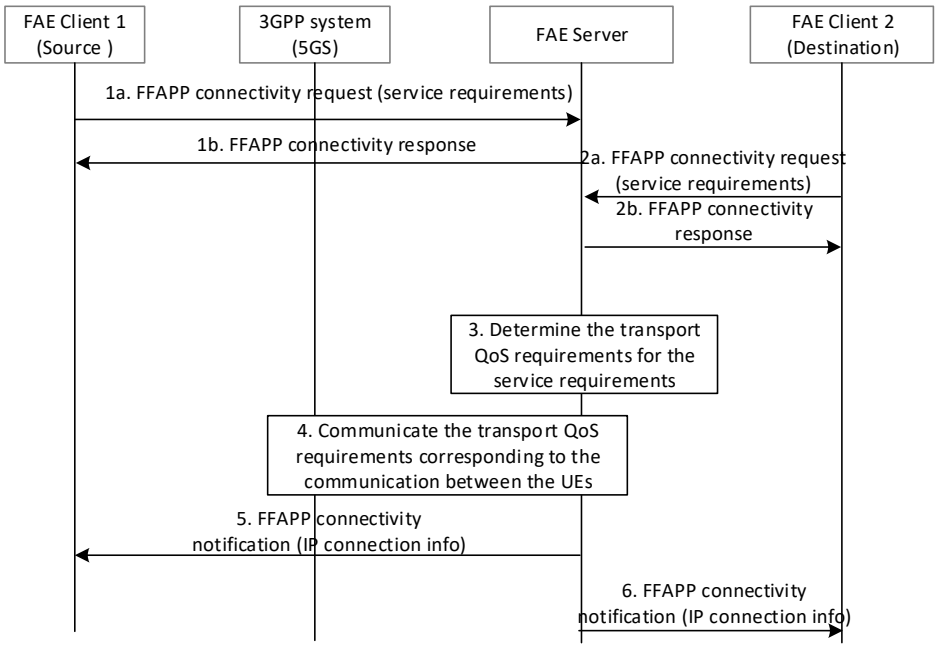

Figure 7.2.1-1: Establishing communication with FF application service requirements

1a. The FAE client 1 sends the FFAPP connectivity request (source identity and IP address, destination identities, service requirements) to the FAE Server. The service requirement from the source includes packet size, packet transmission interval, packet processing latency, allowed packet loss rate/packet loss amount/packet error rate, etc. The destination may be multiple UEs (devices). The identity of source and destination may be the application user identity or the MAC address.

1b. The FAE server determines whether the UE of FAE client 1 is authorized to connect to the destination UEs for direct service communications over FFA-2. If UE of FAE client 1 is authorized to connect to the destination UEs, then a response is provided to the FAE client 1 indicating acceptance of the request.2a. The FAE client 2 sends the FFAPP connectivity request (destination identity and IP address, source identity, service requirements) to the FAE server. The service requirements from the destination includes the transport latency of the packet, processing latency at the destination.

2b. The FAE server determines whether the UE of FAE client 2 is authorized to connect to the destination UEs for direct service communications over FFA-2. If UE of FAE client 2 is authorized to connect to the destination UEs, then a response is provided to the FAE client 2 indicating acceptance of the request.

3. Based on the service requirements received in step 1 and step 2, the FAE server determines the parameters and patterns for direct service connectivity between the UEs (i.e. FFA-2 connectivity) and also the transport requirements, i.e., QoS requirements for the 3GPP system (e.g. 5GS). This step may also include retrieving the direct link status of the UEs (e.g. PDU Session Status, UE reachability, etc. as described in 23.502 [12]). If the FAE server determines that direct service connectivity is not authorized or not possible with the given connectivity requirements, it skips step 4 and proceeds to steps 5 and 6, informing each FAE client accordingly.

NOTE 1: FAE server will process E2E connectivity establishment between FAE client 1 and FAE client 2 only after it receives the request from FAE client 2. There can be several FAE clients (destinations) which will perform step 2 and FAE server will process their E2E connectivity with FAE client 1 (source) as and when the requests are received by the FAE server.

NOTE 2: The FAE server can determine the priority of the E2E connections between FAE client 1 (source) and one or more FAE client 2 (destination) using the service requirements provided to the FAE server by the FAE clients.

4. The FAE server triggers 3GPP system to establish FFA-2 connectivity between the UE of FAE client 1 and UE of FAE client 2 with required QoS as specified in 3GPP TS 23.501 [7].

5. The FAE server sends the FFAPP connectivity notification (connectivity/session information) to FAE client 1 indicating successful establishment of the connectivity. The connectivity/session information may contain the accepted destination identities.

6. The FAE server sends the FFAPP connectivity notification (connectivity/session information) to FAE client 2 indicating successful establishment of the connectivity.

7.2.2 Solution evaluation

This solution addresses key issue#8 and key issue#11 to address application requirement communication and QoS coordination. The solution#2 is a viable technical solution.

7.3 Solution #3: Support UE to UE direct communication in FF application layer

7.3.1 Solution description

Figure 7.3.1-1 illustrates the FF function model to support UE to UE communication in application layer without FF Application Server.

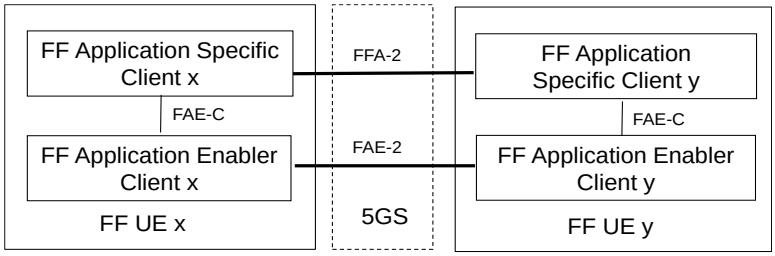

Figure 7.3.1-1: Functional model to support UE to UE direct communication in FF application layer

In order to support FF UE x direct communication to FF UE y in application layer without involvment of FF Application Server, FF application specific client x (which resides on FF UE x) will directly interact with FF application specific client y (which resides in FF UE y) via FFA-2 reference point and the FAE client x (which resides on FF UE x) will directly interact with FAE y (which resides in FF UE y) via FAE-2 reference point.

Note 1: FFA-2 and FAE-2 reference point defined here is Uu interface over 5GS.

Note 2: The defintion of FFA-2 reference point is out of scope of the present document.

7.3.2 Solution evaluation

This solution provides functional model to support UE to UE communication in application layer through 5GS without FF Application Server.

7.4 Void

7.5 Solution #5: Edge deployment within FFAPP

7.5.1 Solution description

This solution corresponds to the key issue #9 - communication service on the Edge deployments.

At UE side, FAE client interacts with the Edge Enabler client via EDGE-5 reference point which described in 3GPP TS 23.558 [10].

In Edge Data network, FAE server interacts with the Edge Enabler Server via EDGE-3 reference point which described in 3GPP TS 23.558 [10].

7.5.2 Solution evaluation

The solution provides a deployment option for FAE client and FAE server considering edge enabler layer.

7.6 Solution #6: Provisioning of FFAPP within Edge Data Network configuration

7.6.1 Solution description

This solution corresponds to the key issue #9 - communication service on the Edge deployments.

The procedure of FFAPP provisioning with Edge Data Network deployment is described as below:

- Pre-condition:

  The FAE client registered to Edge Enabler client. The FAE Server configured with the FF Application Specific Server. The FAE client configured with the FF Application Specific Client; The FAE client registered on the FAE Server with default configuration is optional;

1. The FAE client sends the FFAPP Application Client Profile request to the Edge enabler client via EDGE-5 reference point with related information needed by EEC (which will be defined in 3GPP TS 23.558 [10]).
2. The Edge enabler client will execute the Edge Data Network Configuration provisioning procedure and EAS discovery procedure to get related response information according to the specification of 3GPP TS 23.558 [10].
3. The Edge enabler client on UE sends response information (for example: address of FAE server located in Edge data network) to the FAE client via EDGE-5 reference point. (The response information over EDGE-5 should be defined in 3GPP TS 23.558 [10] and is out of scope of this study.)

Editor's Note: The usage of Edge computing services for FFAPP is FFS.

7.6.2 Solution evaluation

This solution partly addresses the service provisioning and discovery in EDGE deployment, further work is required to solve the EN in clause 7.6.1.

7.7 Solution #7 Geographic location and positioning information support

7.7.1 General

FF UE may use non-3GPP positioning technologies such as GNSS (e.g. Beidou, Galileo, GLONASS, and GPS), Terrestrial Beacon Systems (TBS), sensors (e.g. barometer, IMU), WLAN/Bluetooth-based positioning to get the non-3GPP positioning information.

The FAE capabilities (FAE client and FAE server) can utilize location management (e.g. network location of UEs) service procedures of SEAL to support FF services.

7.7.2 Usage of SEAL location management Information flows

The following information flows of location management service of SEAL as specified in 3GPP TS 23.434 [8] are applicable for the FF applications:

- Enhancements to Location reporting configuration request specified in subclause 9.3.2.0;
- Enhancements to Location reporting configuration response specified in subclause 9.3.2.1;

- Location information report specified in subclause 9.3.2.2;
- Location information request specified in subclause 9.3.2.3;
- Location reporting trigger specified in subclause 9.3.2.4;
- Location information subscription request specified in subclause 9.3.2.5;
- Location information subscription response specified in subclause 9.3.2.6;
- Location information notification specified in subclause 9.3.2.7;

7.7.3 Usage of SEAL location management procedures

The following procedures of location management service of SEAL as specified in 3GPP TS 23.434 [8] are applicable for the FF applications:

- Event-triggered location reporting procedure specified in subclause 9.3.3;
- On-demand location reporting procedure specified in subclause 9.3.4;
- Client-triggered or VAL server-triggered location reporting procedure specified in subclause 9.3.5;
- Location reporting event triggers configuration cancel specified in subclause 9.3.6;
- Location information subscription procedure specified in subclause 9.3.7;
- Event-trigger location information notification procedure specified in subclause 9.3.8;
- On-demand usage of location information procedure specified in subclause 9.3.9;

7.7.4 Enhancements to SEAL location management Information flows

To enable negotiation of positioning method, the location reporting configuration request and location reporting configuration response need to be enhanced as follows:

Table 7.7.4-1, which is based on Table 9.3.2.0-1 in 3GPP TS 23.434 [8], describes the information flow from the location management client to the location management server for requesting the location reporting configuration.

Table 7.7.4-1: Location reporting configuration request

Information element	Status	Description
Identity	M	Identity of the VAL user or identity of the VAL UE.
Supported positioning methods	O	Provides positioning methods supported the VAL UE like non-3GPP positioning technologies such as, GNSS (e.g. Beidou, Galileo, GPS, Glonass), Network-based Assisted GNSS and High-Accuracy GNSS, Terrestrial Beacon Systems, dead-reckoning sensors (e.g. IMU, barometer), WLAN/Bluetooth-based positioning

Table 7.7.4-2, which is based on Table 9.3.2.1-1 in 3GPP TS 23.434 [8], describes the information flow from the location management server to the location management client for the location reporting configuration.

Table 7.7.4-2: Location reporting configuration response

Information element	Status	Description
Identity	M	Identity of the VAL user or VAL group to which the location reporting configuration is targeted or identity of the VAL UE.
Requested location information	O (NOTE 1)	Identifies what location information is requested
Triggering criteria	O (NOTE 1)	Identifies when the location management client will send the location report
Minimum time between consecutive reports	O (NOTE 1)	Defaults to 0 if absent otherwise indicates the time interval between consecutive reports
Preferred positioning method	O (NOTE 2)	Provides the Location Management Server preferred positioning method to be used by the Location Management Client.
NOTE 1: If none of the information element is present, this represents a cancellation for location reporting. NOTE 2: If "Supported position methods" is present in the Location reporting configuration request, then "Required positioning method" shall be one of the supported method.		

Editor's note: How location management server can determine preferred positioning method and provide required location reporting accuracy and other KPIs to location management client are FFS.

SEAL LM function supports to interact with 3GPP Core Network over T8 reference point as specified in 3GPP TS 23.434 [8], clause 9.2.2. With the 5GC unified location service described in 3GPP TS 23.273 [36], the SEAL LM architecture can be enhanced to support T8/N33 reference point so that the 5GC specific location management procedure can be utilized.

The SEAL LM service can expose the desired location quality of service to the Vertical domain users (e.g. FF application specific server). In addition, the SEAL can also utilize the non-3GPP positioning to report more accurate location to the Vertical domain users (e.g. FF application specific server).

The SEAL LM procedures and information flows in 3GPP TS 23.434 [8] can be enhanced (highlighted in ***bold italics***) as follows:

9.2.2 On-network functional model description

Figure 9.2.2-1 illustrates the generic on-network functional model for location management.

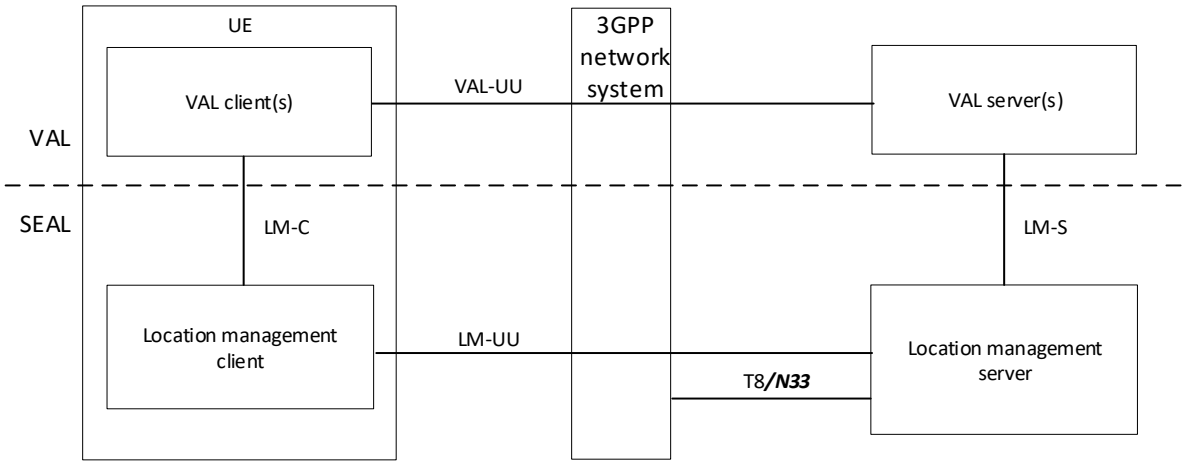

Figure 9.2.2-1: On-network functional model for location management

The location management client communicates with the location management server over the LM-UU reference point. The location management client provides the support for location management functions to the VAL client(s) over LM-C reference point. The VAL server(s) communicate with the location management server over the LM-S reference point.

The location management server communicates with the SCEF***/NEF*** via T8***/N33 reference point*** to obtain location information from the underlying 3GPP network system.

9.3.2.3 Location information request

Table 9.3.2.3-1 describes the information flow from the VAL server to the location management server and from the location management server to the location management client for requesting an immediate location information report.

Table 9.3.2.3-1: Location information request

Information element	Status	Description
Identity list	M	List of VAL users or VAL UEs whose location information is requested
Location QoS	***O***	***Indicate the location quality of service as described in clause 4.1b of TS 23.273 [36].***

9.3.2.5 Location information subscription request

Table 9.3.2.5-1 describes the information flow from the VAL server to the location management server for location information subscription request.

Table 9.3.2.5-1: Location information subscription request

Information element	Status	Description
Identity	M	Identity of the requesting VAL user or VAL UE
Identities list	M	List of VAL users or VAL UEs whose location information is requested.
Time between consecutive reports	M	It indicates the interval time between consecutive reports
Location QoS	***O***	***Indicate the location quality of service as described in clause 4.1b of TS 23.273 [36].***

9.3.8 Event-trigger location information notification procedure

Figure 9.3.8-1 illustrates the high level procedure of event-trigger usage of location information. The same procedure can be applied for location management client and other entities that would like to subscribe to location information of VAL user or VAL UE. This procedure is also used for obtaining latest UE's location for tracking purpose.

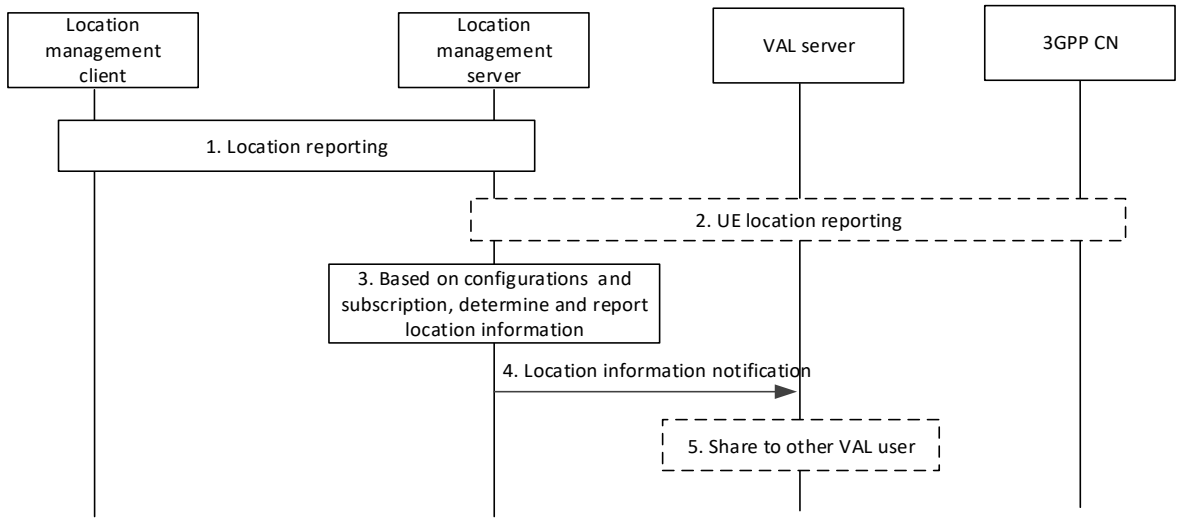

Figure 9.3.8-1: Event-trigger usage of location information procedure

1. The location management server receives the latest location information of the UE as per the location report procedure described in clause 9.3.3.3.

2. The location management server may optionally receive the location information of the UE from 3GPP core network.

3. Based on the configurations, e.g., subscription, periodical location information timer, location management server is triggered to report the latest user location information to VAL server. The location management server determines the location information of UE as received in steps 1 and 2. ***The Location management server may report the location to the VAL server considering the location information received via non-3GPP positioning technologies (e.g. GNSS, bluetooth), for instance, to improve the location accuracy.***

4. The location management server send the location information report including the latest location information of one or more VAL users or VAL UEs to the VAL server.

5. VAL server may further share this location information to a group or to another VAL user or VAL UE.

NOTE: For other entities, the step 5 can be skipped if not needed.

9.3.9 On-demand usage of location information procedure

The VAL server can request UE location information at any time by sending a location information request to the location management server, which may trigger location management server to immediately send the location report.

Figure 9.3.9-1 illustrates the high level procedure of on demand usage of location information. The same procedure can be applied for location management client and other entities that would like to subscribe to location information of VAL user or VAL UE.

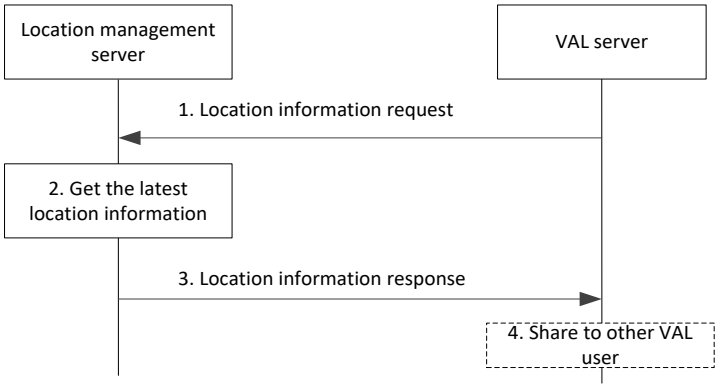

Figure 9.3.9-1: On-demand usage of location information procedure

1. VAL server sends a location information request to the location management server.
2. The location management server acquires the latest location of the UEs being requested, by triggering an on-demand location report procedure as described in subclause 9.3.4, ***and/***or from PLMN operator.
3. Then, location management server immediately sends the location information report including the latest location information acquired of one or more VAL users or VAL UEs. ***The Location management server may report the location to the VAL server considering the location information received via non-3GPP positioning technologies (e.g. GNSS, bluetooth), for instance, to improve the location accuracy.***
4. VAL server may further share this location information to a group or to another VAL user or VAL UE.

NOTE: For other entities, the step 3 can be skipped if not needed.

7.7.5 Solution evaluation

This solution utilizes and enhances the SEAL location management service to support FFAPP geographic location and high accuracy positioning requirements. This solution does not support positioning method with ms-level latency and absolute and relative positioning which listed in open issues of Key issue 2.

7.8 Solution #8: QoS monitoring

7.8.1 Solution description

This solution addresses Key issue 5 - QoS monitoring.

QoS monitoring is a critical requirement for many FF applications.

The issue to address here via the NEF, according to the procedures defined in 3GPP TS 23.502 [12] clause 4.15. NEF supports APIs of exposure of network events, analytics for QoS monitoring.

The detail procedures over NEF Northbound Interface are defined in 3GPP TS 29.522 [11] clause 4.4:

- Procedures for setting up an AF session with required QoS, which defines QoS monitoring event (QOS_MONITORING) within "QoSMonitoring_5G" feature
- Procedures for analytics information exposure, which defines analytics event (QOS_SUSTAINABILITY) within "QoS_Sustainability" feature

7.8.1.1 QoS monitoring procedure

Pre-conditions:

1. The FF UE has already registered, configured, provisioned.
2. The FF UE has an established connection to 5G network.

The procedure for QoS monitoring is illustrated in figure 7.8.1.1-1.

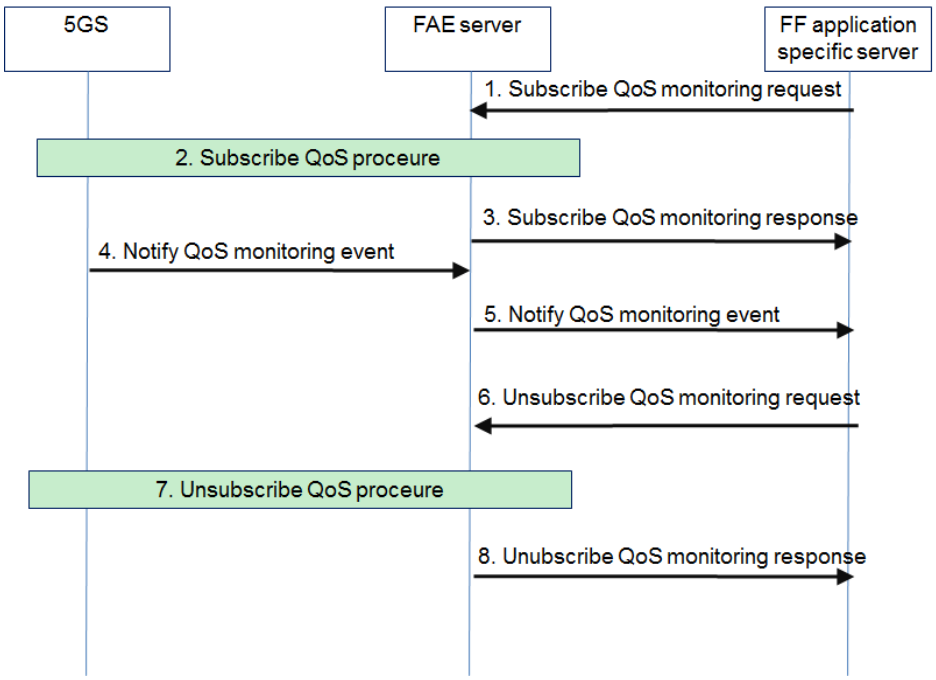

Figure 7.8.1.1-1: QoS monitoring procedures

1. The FF application specific server sends a QoS monitoring subscribe request to the FAE server.
2. The FAE server interacts with NEF to subscribe to QoS monitoring events, including:
   - QOS_MONITORING, supported by AsSessionWithQoS API of 3GPP TS 29.522 [11]
   - QOS_SUSTAINABILITY, supported by AnalyticsExposure API API of 3GPP TS 29.522 [11]
3. The FAE server sends a QoS monitoring subscribe response to the FF application specific server.
4. When QoS monitoring event is triggered, NEF sends a QoS monitoring notification to the FAE server.
5. The FAE server determines the QoS monitoring event information to send to the FF application specific server. The transport related information received from 3GPP system should be translated to application related information by the FAE server.

   NOTE: Steps 4 and 5 are repeated when QoS monitoring events occur.
6. When the FF application specific server decides to unsubscribe for the QoS monitoring, the FF application specific server sends a QoS monitoring unsubscribe request to the FAE server.
7. The FAE server interacts with NEF to unsubscribe from QoS monitoring events.
8. The FAE server sends a QoS monitoring unsubscribe response to the FF application specific server.

7.8.2 Solution evaluation

This solution is technically viable as it reuses capabilities already defined and no new requirements related to that functionality have been identified. It is recommended to use a common solution for QoS monitoring in SEAL.

7.9 Solution #9: 5GLAN group management

7.9.1 Solution description

This solution function addresses the Key issue #6.

7.9.1.1 General

In factory network, the FF UE is using 5G LAN-type of services, when a FF UE is in a group, which includes 5GLAN related network information.

The FAE capabilities (FAE client and FAE server) utilize the group management service procedures (e.g. creation, group membership update) of SEAL based on the 5GLAN group configuration information provided by the FF application specific layer.

7.9.1.2 Information flows

The following information flows of group management service of SEAL as specified in 3GPP TS 23.434 [8] are applicable for the FF applications:

- Group creation request from the SEAL group management client to the SEAL group management server, information specified in table 10.3.2.1-1;
- Group creation response from the SEAL group management server to the SEAL group management client, information specified in table 10.3.2.2-1;
- Group creation notification from the SEAL group management server to the FAE server, information specified in table 10.3.2.3-1;
- Group information query request from the SEAL group management client to the SEAL group management server, specified in subclause 10.3.2.4;
- Group information query response from the SEAL group management server to the SEAL group management client specified in subclause 10.3.2.5;
- Group membership update request from the SEAL group management client to the SEAL group management server, information specified in table 10.3.2.6-1;
- Group membership update response from the SEAL group management server to the SEAL group management client, information specified in table 10.3.2.7-1;
- Group membership notification from the SEAL group management server to the FAE server, information specified in table 10.3.2.8-2;
- Group deletion request from the SEAL group management client to the SEAL group management server, information specified in table 10.3.2.9-1;
- Group deletion response from the SEAL group management server to the SEAL group management client, information specified in table 10.3.2.10-1;
- Group deletion notification from the SEAL group management server to the SEAL group management client and FAE server, information specified in table 10.3.2.11-1;
- Store group configuration request from the SEAL group management client to the SEAL group management server, information specified in table 10.3.2.18-1;
- Store group configuration response from the SEAL group management server to the SEAL group management client, information specified in table 10.3.2.19-1;
- Get group configuration request from the SEAL group management client to the SEAL group management server, specified in subclause 10.3.2.20;

- Get group configuration response from the SEAL group management server to the SEAL group management client, specified in subclause 10.3.2.21;

- Subscribe group configuration request from the SEAL group management client to the SEAL group management server, information specified in table 10.3.2.22-1;

- Subscribe group configuration response from the SEAL group management server to the SEAL group management client, information specified in table 10.3.2.23-1;

- Notify group configuration request from the SEAL group management server to the SEAL group management client, information specified in table 10.3.2.24-1;

- Notify group configuration response from the SEAL group management client to the SEAL group management server, information specified in table 10.3.2.25-1;

- Group announcement from the SEAL group management server to the SEAL group management client, information specified in table 10.3.2.28-1;

- Group registration request from the SEAL group management client to the SEAL group management server, information specified in table 10.3.2.29-1;

- Group registration response from the SEAL group management server to the SEAL group management client, information specified in table 10.3.2.30-1;

- Group de-registration request from the SEAL group management client to the SEAL group management server, information specified in table 10.3.2.32-1;

- Group de-registration response from the SEAL group management server to the SEAL group management client, information specified in table 10.3.2.33-1;

- Identity list notification from the SEAL group management server to the SEAL group management client and to the FAE server, information specified in tables 10.3.2.31-1 and tables 10.3.2.31-2 respectively;

- Configure VAL group request from the FAE server to the SEAL group management server with FF 5GLAN group configuration information, information specified in table 7.9.1.2-1 as below;

Table 7.9.1.2-1, which is based on Table 10.3.2.26-1 in 3GPP TS 23.434 [8], describes the information flow for configure VAL group request from a VAL server to the SEAL group management server.

Table 7.9.1.2-1: Configure VAL group request

Information element	Status	Description
Requester Identity	M	The identity of the VAL server performing the request.
VAL group ID	M	The group ID used for the VAL group.
VAL group description	M	Information related to the VAL group e.g. group definition including policy, group size, group leader.
VAL service ID list (see NOTE)	O	List of VAL services whose service communications are to be enabled on the group.
Geo ID list (see NOTE)	O	List of geographical areas to be addressed by the group.
Identity list (see NOTE)	O	List of VAL UE IDs who are member of the group.
Identity list subscription	O	Indicates interest to receive notifications of newly registered VAL UE IDs.
NOTE: At least one of these IEs shall be present.		

- Configure VAL group response from the group management server to the FAE server, specified in subclause 10.3.2.27;

The usage of the above information flows is clarified as below:

- The identity list is the list of FF UE IDs.

  -- During group creation the identity list contains the list of FF UE IDs that are part of the group to be created. If the group member list is empty, an empty group is created; and

- The VAL group ID is the FF 5GLAN group ID, which maps to the External Group ID in 3GPP TS 23.502 [12] clause 4.15.3b;
- The identity is the FF UE ID;
- The VAL server is the FAE server;
- The VAL group description shall include description of the group indicating 5G LAN-Type service and communication type (IP or Ethernet) for the group communication. 5G LAN-Type service is defined in 3GPP TS 23.501 [7];
- The VAL service ID list should include at least the FF service identity;

7.9.1.3 Procedures

The following procedures of group management service of SEAL as specified in 3GPP TS 23.434 [8] are applicable for the FF applications:

- Group creation from the FAE server to the group management server with group creation request and group creation response;
- Group information query from the group client to the group management server with group information query request and group information query response;
- Group membership update from the FAE server to the group management server with group membership update request and group membership update response;
- Group membership notification from the group server to the group management client;
- Group deletion from the FAE server to the group management server with group deletion request and group deletion response;
- Retrieve group configurations from the group client to the group management server with get group configuration request and get group configuration response;
- Configure VAL group from the FAE server to the group management server with Configure VAL group request and Configure VAL group response

7.9.1.4 Required SEAL group management enhancements

SEAL group management server shall enable a VAL server (FAE server) to create, update, delete, subscribe to changes of a 5GLAN group. 5GLAN group is defined in 3GPP TS 23.501 [7]. The SEAL group management client and the VAL server shall be able to identify that a group managed by the SEAL server is used for 5G LAN-Type service.

For group management procedures pertaining to a 5GLAN group the SEAL group management server shall use dynamic 5G VN group management procedures exposed by NEF via the N33 reference point, as specified in TS 23.501 [7] clause 5.29.2 and in TS 23.502 [12] clause 4.15.6.

5GLAN (also referred to as 5G VN) group data is specified in TS 23.502 [12] clauses 4.15.6.3b and 4.15.6.3c. The SEAL group management server shall use the VAL service identity to derive the 5G VN group data such as DNN, S-NSSAI, etc.

The SEAL group management may use the procedures of the event monitoring of PDN Connectivity Status specified in 3GPP TS 23.502 [12] clause 4.15.3.2.3 to keep track of the connectivity status of the group member UEs, e.g. to detect VAL UE registration/de-registration to/from the group.

7.9.1.5 5GLAN group creation and join procedure

This procedure is based on the Group announcement and join procedure in 3GPP TS 23.434 [8] clause 10.3.8. In this procedure the VAL server is composed of the FAE server and the FF application specific server.

Pre-conditions:

1. The SEAL group management clients, SEAL group management server, VAL server and the VAL clients belong to the same VAL system.

2. The VAL server is aware of the users' identities and is authorized to form a VAL group for 5G LAN-Type communication.

3. The VAL clients (at the VAL UEs) belong to the same 5GLAN (5G-VN) group.

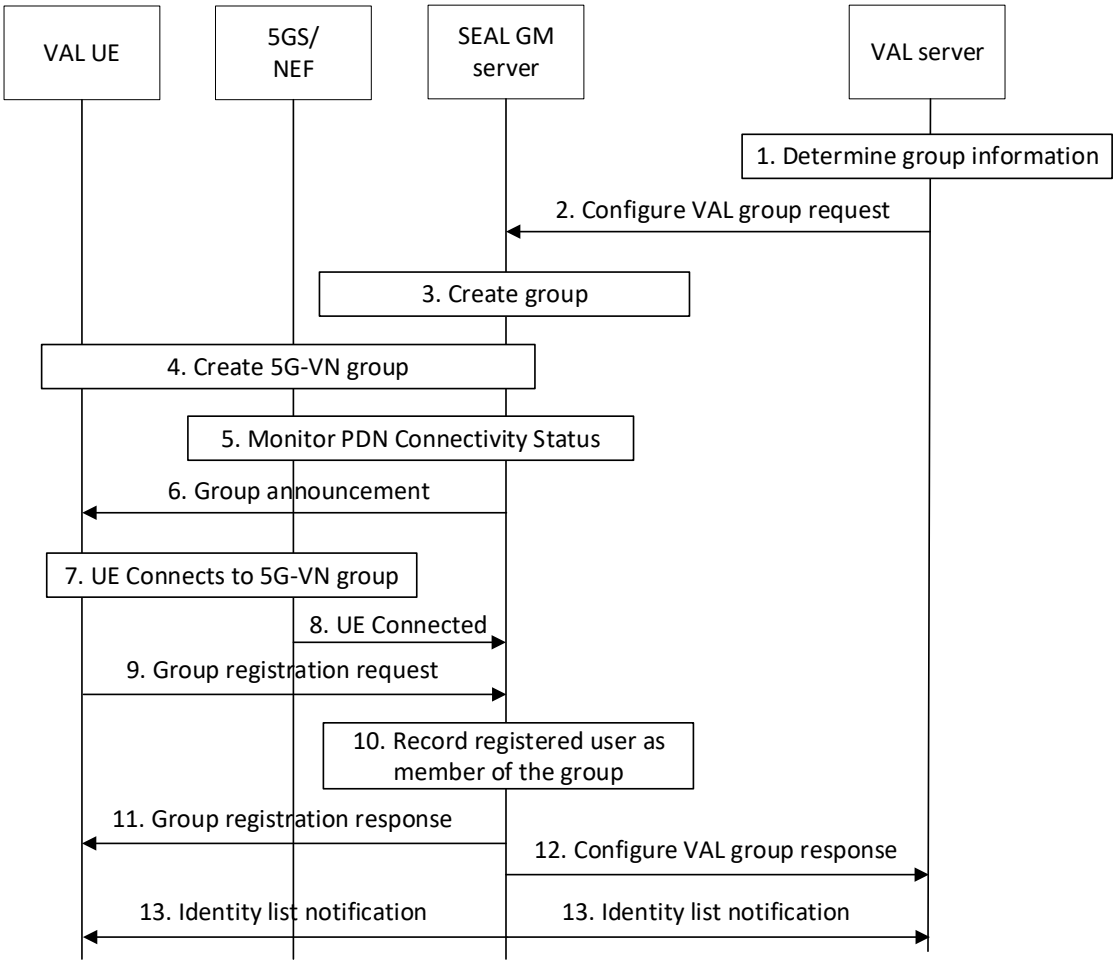

Figure 7.9.1.5-1: Procedure for creating a VAL group for 5G LAN-Type communication.

1. The VAL server determines group information and the identity list to which the group announcement shall be sent. The decision can be based on the list of authorized UEs and other criteria such as requirement for 5G LAN-Type communication service.

2. The VAL server requests the SEAL group management server to configure a new VAL group for 5G LAN-Type communication service providing a VAL Group ID, a list of VAL UEs and a list of VAL services.

3. The SEAL group management server creates an empty group and determines that the group is for 5G LAN-Type communication, based on the information provided in the Configure VAL group request. The SEAL group management server determines 5GLAN group data for the VAL server.

4. The SEAL group management server creates a 5GLAN group in the 5GS via N33 using the dynamic group management procedures specified in 3GPP TS 23.501 [7] clause 5.29.2 and 3GPP TS 23.502 [12] clause 4.15.6. The 5GS delivers 5G VN group configuration information (DNN, S-NSSAI, PDU session type) to the VAL UEs for each GPSI that belongs to the 5GLAN group. The 5G VN group configuration information is delivered in the UE Route Selection Policy (URSP) from the 5GS to the VAL UEs using the UE Configuration Update procedure for transparent UE Policy delivery as described in TS 23.502 [12] clause 4.2.4.3.

5. The SEAL group management server may subscribe to PDN Connectivity Status events via N33 using the procedures specified in 3GPP TS 23.502 [12] clause 4.15.3.2.3 in order to be notified of the connectivity status of the VAL UEs of the 5GLAN group.

NOTE 1: The SEAL group management server may use PDN Connectivity Status events e.g. to determine VAL UE's registration state in the group.

6. The SEAL group management server announces the VAL group to the SEAL group management client at the VAL UEs, including the DNN and communication type (IP or Ethernet) corresponding to the 5GLAN group,

NOTE 2: The SEAL group management server can decide to use the Application Trigger service provided by the NEF described in 3GPP TS 23.502 [12] clause 5.2.6.5 for group announcement to the group management client or to use the group announcement already specified in 3GPP TS 23.434 [8].

7. The SEAL group management client in the VAL UEs determines the group to be a 5GLAN group and triggers establishment of a PDU session corresponding to the 5GLAN group.

8. If the SEAL group management server subscribed to PDN Connectivity Status events in step 5, it is notified once the VAL UE establishes a PDU session to the 5GLAN group. Receiving this event is sufficient for the SEAL group management server to determine that the VAL UE is a member of the group.

9. The SEAL group management client at the VAL UEs registers to VAL group communication using the VAL Group ID.

10 The SEAL group management server records the users who have registered to be the members of the group.

NOTE 3: Step 10 may occur as a result of Step 8.

11. The SEAL group management server sends a VAL group registration response to the SEAL group management clients.

12. The SEAL group management server sends a configure VAL group response to the VAL server.

NOTE 4: Step 12 may occur any time after Step 6.

13. The SEAL group management server sends identity list notification about the newly registered users. The SEAL group management client in the VAL UEs may inform the VAL client about the updated identity list.

7.9.2 Solution evaluation

This solution provides enhancements to the SEAL group management service to handle 5GLAN groups based on 5G core network capabilities already specified in Rel-16 3GPP TS 23.501 [7] and Rel-16 3GPP TS 23.502 [12]. This solution addresses the gaps described in key issue #6.

7.10 Solution #10: QoS monitoring for TSC services

7.10.1 Solution description

This solution addresses KI#5 on QoS monitoring.

Monitoring of QoS for time sensitive communication (TSC) services is a critical requirement for many FF applications.

QoS monitoring to assist URLLC is specified in clause 5.33.3 of TS 23.501 [7], with per flow monitoring mechanism specified in clause 5.33.3.2.

The issue to address here is whether the QoS monitoring capabilities provided by the NEF should be used by the FAE layer directly or via the Service Enabler application layer (SEAL), as according to the concepts defined in 3GPP TS 23.434 [8]. Due to the fact that QoS monitoring is not specific to FF applications but applicable for wider range of vertical applications, it is more suitable to enhance SEAL to support this functionality.

SEAL Network Resource Management service enabler specifies APIs to request reservation, modification, and release of network resources, including QoS resources, see clause 14 in 3GPP TS 23.434 [8] and clause 5.5 in 3GPP TS 29.549 [14]. It is therefore proposed to enhance the Network Resource Management service enabler with the QoS monitoring functionality.

The SEAL Network Resource Management server interacts with NEF via N33 to obtain the relevant QoS monitoring information from the 5GS.

7.10.2 Subscribe/unsubscribe to/from QoS monitoring events for an established connection

The procedure to subscribe/unsubscribe to/from QoS monitoring events is shown in figure 7.10.2-1.

Pre-conditions:

- The FF UE has an established connection in the 5GS

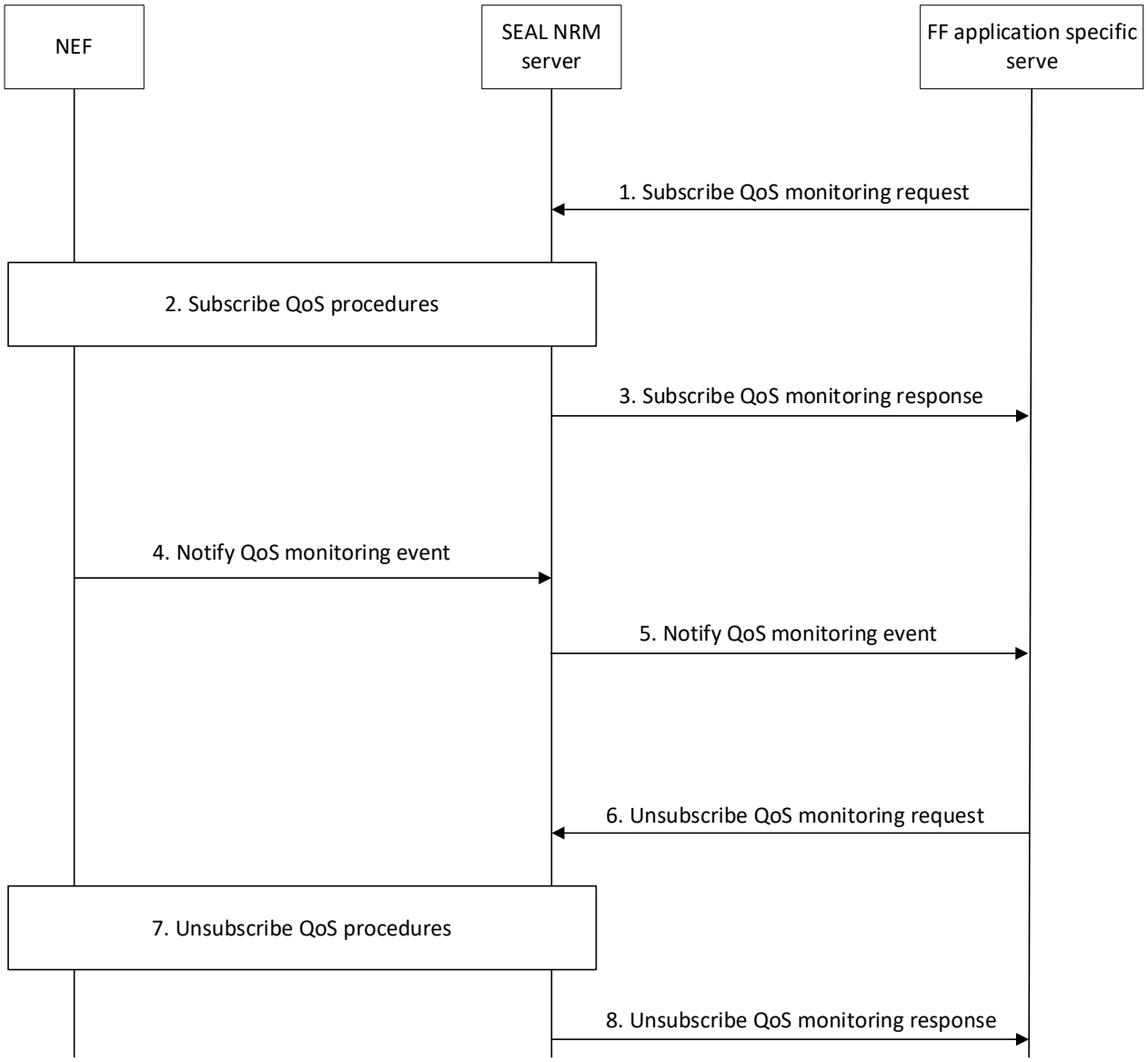

Figure 7.10.2-1: Subscribe/unsubscribe QoS monitoring procedures

1. The FF application specific server sends a QoS monitoring subscribe request to the SEAL NRM server either in conjunction with a request for network resources requiring QoS or when the QoS connection is already established.

2. The SEAL NRM server interacts with the NEF to establish a QoS monitoring subscriptions. The NRM server uses the NEF procedures for the AFsessionWithQoS described in clause 5.2.6.9 of 3GPP TS 23.502 [12] and the NEF procedures for the AnalyticsExposure described in clause 5.2.6.16 of 3GPP TS 23.502 [12] and in particular the UE Communication Analytics (see clause 6.7.3 of 3GPP TS 23.288 [19]). In those interactions the

SEAL NRM server determines QoS parameters to be measured (e.g. DL, UL or round trip packet delay, UL/DL data rate, traffic volume), including, but not limited:

- frequency of reporting (event triggered, periodic, or when the PDU Session is released):
  a) if the reporting frequency is event triggered:
     i) the corresponding reporting threshold to each QoS parameter;
     ii) minimum waiting time between subsequent reports;
  b) if the reporting frequency is periodic, the reporting period.

3. The SEAL NRM server sends a QoS monitoring subscribe response to the FF application specific server.
4. When QoS monitoring event is triggered and the SEAL NRM server is notified by the NEF. The SEAL NRM server may coordinate and combine the information from the NEF notifications before sending a notification to the FF application specific server.
5. The SEAL NRM server notifies the FF application specific server about the QoS monitoring event.

NOTE: Steps 4 and 5 are repeated when QoS monitoring events occur.

6. When the FF application specific server decides to unsubscribe for the QoS monitoring, the FF application specific server sends a QoS monitoring unsubscribe request to the SEAL NRM server.
7. The SEAL NRM server interacts with the NEF to terminate the related QoS monitoring subscriptions.
8. The SEAL NRM server sends a QoS monitoring unsubscribe response to the FF application specific server.

7.10.3 Solution evaluation

This solution enhances the SEAL Network Resource Management service enabler with QoS monitoring and uses the exposure of QoS monitoring procedures provided via NEF as already specified in Rel-16. It provides common support for QoS monitoring for FFAPP and other verticals. It is a technically viable solution to address KI #5.

7.11 Solution #11: Establishing communication connectivity between FF Application Specific Clients with FF application service requirements

7.11.1 Solution description

This solution corresponds to the key issue #8 on communication of FF application requirements with 5GS and key issue#11 on QoS coordination.

In this solution, a FAE client and FAE server (acting as an AS) exchange context information allowing for the desired service requirements (e.g. data rate) for the communication amongst the FF application specific clients to be derived. The FAE server adaptively triggers retrieval of context and establishment of direct service connectivity, e.g. when the two UEs are close to each other. Note that service connectivity among FF application specific clients is established over the FFA-2 reference point, without device-to-device direct radio connectivity (e.g. PC 5) requirement.

The procedure for establishing FFA-2 service communication with FF application specific clients service requirements provided via the FAE Clients is as illustrated in figure 7.11.1-1.

Pre-conditions:

- FAE client 1 and FAE client 2 are provided configuration information for the FF application specific clients served e.g. connectivity requirements, etc.
- FAE client 1 and FAE client 2 are configured with the information of the FAE server and have registered (e.g. using clause 7.4 procedures). The information is provided via pre-configuration or registration to the FAE server

includes FAE client capabilities, security information, etc. Upon registration, FAE client 1 and FAE client 2 subscribe to connectivity notifications.

- Pre-processing determines that connectivity between FF application specific client 1 to FF application specific client 2 via the FFA-2 reference point is required. Service requirements and destination information for this connection have been provided, e.g. via discovery.

NOTE: The preconditions above rely upon procedures (e.g. registration, discovery) detailed as part of other solutions.

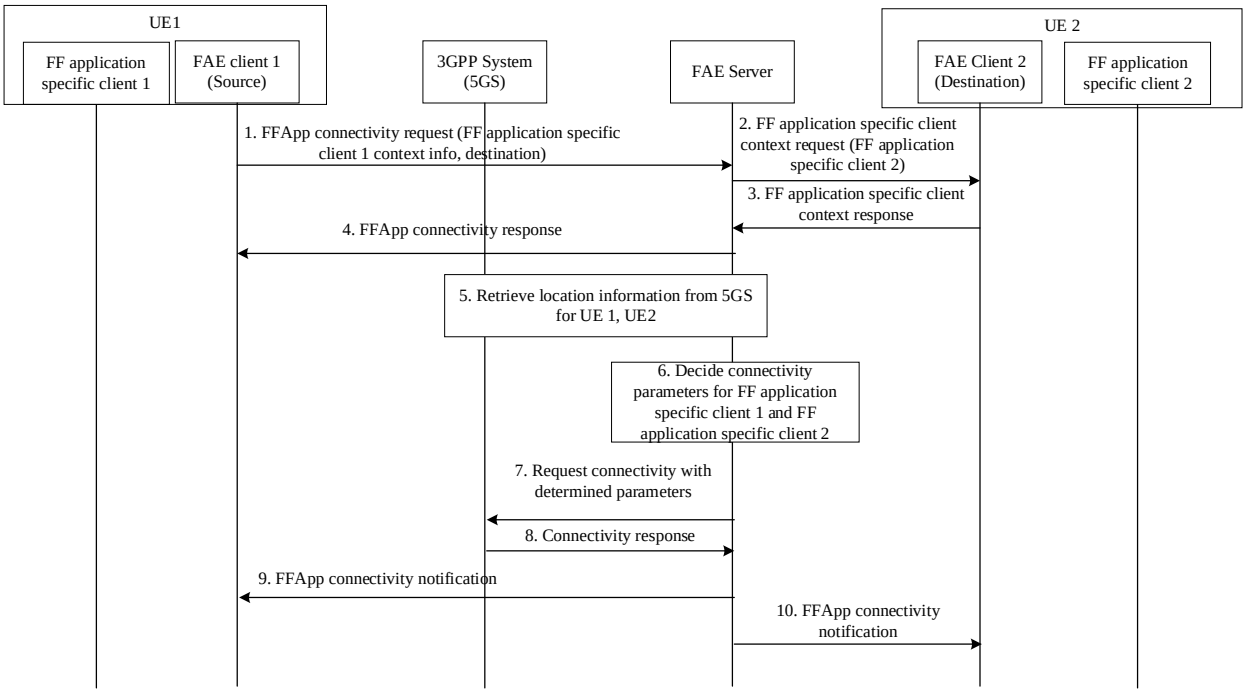

Figure 7.11.1-1: Establishing communication connectivity between FAE Clients with FF application service requirements

1. The FAE Client 1 sends the FFAPP connectivity request (source identity and IP address, destination identities, service requirements) to the Future Factory Enabler Server (FAE server) to establish connectivity for FF application specific client 1 on UE 1. The destination FF application specific client(s) may be hosted on one or multiple UEs (devices). The identity of the source and of the destination may be provided as the application user identity or the MAC address.

2. The FAE server determines whether FF application specific client 1 is authorized to connect to FF application specific client 2 for direct service communications over FFA-2. If FF application specific client 1 is authorized to connect to FF application specific client 2, the FAE server contacts the FAE client 2 to retrieve its FF application specific client 2 context information. This step can be skipped if the FAE server is already aware of FF application specific client 2's context information.

   Editor's Note: It is FFS how FAE server determines whether FF application specific client 1 is authorized to connect to FF application specific client 2 for direct service communications over FFA-2.

3. The FAE client 2 determines whether context information is to be provided for establishing connectivity for FF application specific 2 to FF application specific 1. FAE client 2 makes this determination based on FF application specific client 1 information provided in the request, pre-provisioned information (e.g. policies) and its context (e.g. location, time, etc.) If FAE client 2 determines that context information is to be provided, it responds to FAE server and includes the context information for FF application specific client 2.

NOTE: The signaling and functionality for handling the cases when FAE client 2 will be temporarily unavailable for establishing the direct service connection are implementation dependant.

4. The FAE server responds to the FFAPP connectivity request in step 1.

5. The FAE server retrieves location information of UE 1 and UE 2 hosting the two FF application specific clients respectively. This step may also include a request for direct link status (e.g. PDU Session Status, UE reachability, etc. as described in 23.502 [12]). This step may be skipped if the FAE server is already aware of UE 1's and UE 2's location information or if there are no location requirements for establishing the FF application specific client 1 to FF application specific 2 direct service connectivity.

NOTE: If SEAL is used, location information may be obtained from the SEAL location management server. Alternatively, Location Reporting monitoring as described in 23.502[12] may be used.

6. The FAE server takes FF application specific client 1's and FF application specific client 2's context information, their connectivity requirements, location information, and network context as input, checks connectivity service policies, and determines the parameters and patterns for direct service connectivity between the FF application specific clients (i.e. FFA-2 connectivity). The FAE server may also determine transport requirements, e.g. QoS requirements, for the 3GPP system (e.g. 5GS).

   If the FAE server determines that direct service connectivity is not possible with the given connectivity requirements, it skips step 7 and proceeds to steps 9 and 10, informing each FAE client accordingly. If the FAE server determines that direct service connectivity is not authorized or not possible with the given connectivity requirements, it skips step 7 and proceeds to steps 9 and 10, informing each FAE client accordingly.

7. The FAE server may request the 3GPP system to establish or modify the 3GPP system level connectivity that enables the application connection between FF application specific client 1 and FF application specific client 2 e.g. via modification of existing radio bearers. FAE server provides the necessary information (e.g. identifiers of FF application specific client 1 and FF application specific client 2, transport requirements) in this request message.

   Editor's Note: If SEAL is used, the procedure for communicating FF application service requirements from FAE server to the 3GPP system may utilize enhanced NRM server functionality. It is FFS whether NRM server functionality may be enhanced to support translating FF application service requirements to 3GPP network requirements.

8. The FAE server receives a response from the 3GPP system indicating whether the requested connectivity in Step 6 has been successfully established or modified.

9. The FAE server notifies FAE client 1 of the established connection including its properties such as a FFA-2 direct service connection identifier, duration, etc.

10. The FAE server notifies the FAE client 2 of the established connection including its properties such as a FFA-2 direct service connection identifier, duration, etc.

    Editor's Note: Traffic routing between FAE client 1 and FAE client 2 over FFA-2 is FFS.

7.11.2 Solution evaluation

This is a viable technical solution for key issue #8 and key issue #11. The FAE server translates the FF application specific requirements for connectivity to the 3GPP network based on FAE client requests.

7.12 Solution #12: Private Slice

7.12.1 Solution description

7.12.1.1 General

This solution corresponds to the Key issue #1 - Use of network slicing for FFAPP and Key Issue 13: Capability Exposure related to Private Slice Network Status.

3GPP TS 22.261 [2] defines private slice is a dedicated network slice deployment for the sole use by a specific third-party and describes to operate a hosted non-public network and private slice(s) of its PLMN associated with the hosted non-public network in a combined manner. It meanings that private slice is belong to PLMN.

3GPP TS 22.261 [2] specifies that the 5G network shall provide suitable APIs to allow a trusted third-party to get the network status information of a private slice dedicated for the party, e.g. the network communication status between the slice and a specific UE.

3GPP TS 23.501 [7] defines the 5G System architecture and high level features, which not includes specific solution or feature for private slice.

3GPP TS 28.541 [17] specifies the Information Model and Solution Set for the Network Resource Model (NRM) definitions of NR, NG-RAN, 5G Core Network (5GC) and network slice, which not includes specific Information Model and Solution Set for private slice.

3GPP SA2 has already start study on enhanced support of non-public networks and enhancement of network slicing in Release 17, which not includes specific solutions for private slice.

Currently, the solution for private slice is no different with other network slices.

SA2 defines network slice information (Slice load level related network data analytics, UE Communication Analytics which defined in 3GPP TS 23.288 [19]) exposed by NEF through AnalyticsExposure API which defined in 3GPP TS 29.522 [11].

Network slice information also can through SA5 NMS to get, monitor, config. Exposure governance management function (EGMF) in 3GPP TS 28.533 [18] is management function in network function model with the role of management service exposure governance, it is similar as NEF.

Expose Network slice information is a common functionality for all verticals (and not only V2X and FF), so SEAL should to enhance to support.

The FAE server can utilize Network Resource Management of SEAL to support to get the network status information of a private slice (e.g. the network communication status between the slice and a specific UE). Which needs to enhance the existing Network Resource Management service enabler by adding acquirement of private slice network status information through NEF AnalyticsExposure API or Exposure Governance Management Function (EGMF) by 3rd party (e.g. from vertical industry) which defined in 3GPP TS 28.533 [18].

NOTE 1: How SEAL support NEF is out of scope of the present document.

NOTE 2: How SEAL support EGMF is out of scope of the present document, the solution is in the scope of SA5 and SEAL. Details of EGMF management capability exposure governance in 3GPP TS 28.533 [18] is FFS by SA5.

7.12.1.2 Acquirement of private slice network status information procedure

The procedure for acquirement of private slice network status information is illustrated in figure 7.12.1.2-1.

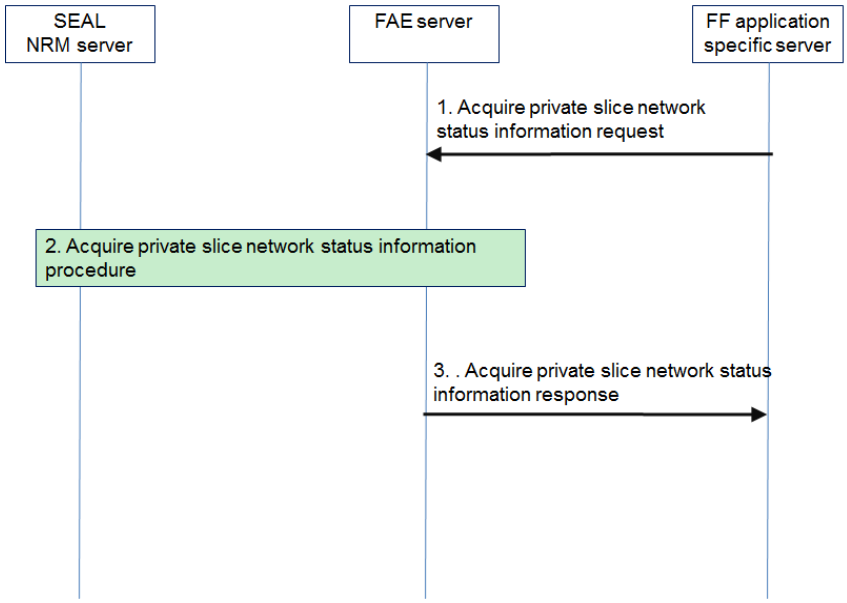

Figure 7.12.1.2-1: Acquirement of private slice network status information procedures

1. The FF application specific server sends an Acquire private slice network status information request to the FAE server.

2. The FAE interacts with the SEAL Network Resource Management server to acquire private slice network status information. The SEAL Network Resource Management server acquires private slice network status information, including, but not limited:

   a) The SEAL Network Resource Management server interacts with NEF by AnalyticsExposure API to fulfil the operation (not shown in the sequence). In that interaction the SEAL NRM server acquirement private slice network status information (e.g. slice specific UE_COMM as described in 3GPP TS 29.522 [11]).

   b) The SEAL Network Resource Management server interacts with EGMF to fulfil the operation (not shown in the sequence). In that interaction the SEAL NRM server acquirement private slice network status information (e.g. pduSessionType, NetworkSlice as described in 3GPP TS 28.541 [17]).

3. The FAE server sends an Acquire private slice network status information response to the FF application specific server.

NOTE 3: How FAE interacts with the SEAL Network Resource Management server is out of scope of the present document, the solution need SEAL further study.

Editor's note: whether NRM server or a new SEAL service is required to support slice status reporting is FFS.

7.12.2 Solution evaluation

This solution depends on how SEAL to support NEF or EGMF and acquire private slice network status information. The specification of such a mechanism, therefore, will be required to be used as the baseline when the solution described in this clause is addressed during the normative work.

7.13 Solution #13: Application-triggered slice re-mapping for FF applications

7.13.1 Solution description

This solution provides a mechanism for enabling the FAE server to translate the adaptation of the service requirements / profile, as triggered by the FF application specific server or client, to a network slice re-mapping.

7.13.1.1 General

This solution provides a mechanism to allow the FAE server to perform slice re-mapping for a FF application and the involved UEs, as triggered by a change of the application requirements. This mechanism assumes that the GST parameters and the per UE slice subscriptions (running the FF application) are known at the FAE server by OAM (according to TS 28.533 [18] slice management information can be exposed to 3rd party via EGMF).

The trigger for the mapping is the FF application specific server (or FAE client) request to FAE server for a new service profile (e.g. URLLC, eMBB, MIoT) for the FF application. This may be for example, due to change of communication model, Remote vs Local C2C, one or more UEs moving to an area where current service requirements need to be change, different FF application to service mapping, etc.

The FAE server determines an application to slice mapping, based on the requested service profile, the slice capabilities, the UE subscriptions and the GST parameters (these are assumed to be available at the by OAM). The FAE server sends to the SEAL/NRx server the (re-) mapping required to a different slice; and SEAL/NRx server in-turn provides an AF request to re-map the users within the FF application to different slice, by triggering the update of the UE policies.

7.13.1.2 Procedure

Pre-condition1: Slice#1 and Slice#2 have already been established. UEs of App#A have registered with the network and connected to Slice#1 (based on the URSP rules which are configured to the UE by the PCF (TS 23.501 [7], 23.503 [15])).

Pre-condition 2: Slice information, such as GST parameters and slice subscriptions are received at the FAE server by the OAM (by consuming Management APIs via EGMF, as in TS 28.533 [18]).

Pre-condition 3: FF application specific server has requested FAE server to manage the App#A to slice mapping. Following, the FAE server maps App#A (and the FF UEs within App#A) to Slice #1 (based on received slice information) and stores the mapping information.

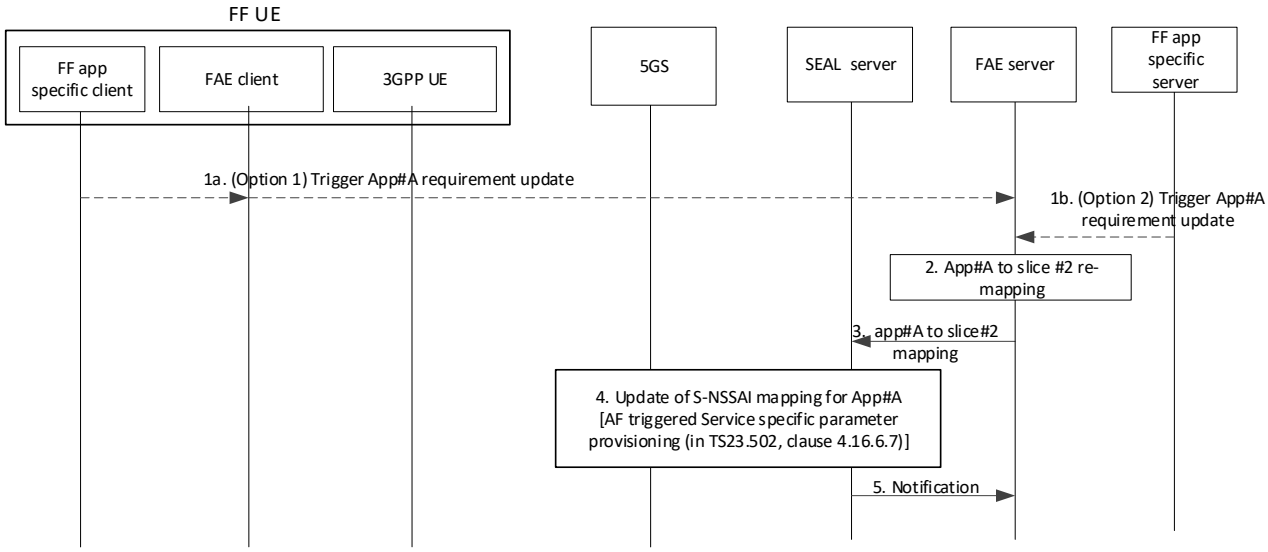

Figure 7.13.1.2-1: FF application to slice mapping by FAE layer

1. A trigger event is captured at the application layer. Two options are possible:

   1a. The FF application specific client of the FF-UE needs to adapt the app#A to service profile mapping, e.g. due to QoE adaptation, UE mobility, communication model change. Then, the FF application specific client sends to FAE server via the FAE client an updated service profile trigger event report for requesting the adaptation of the service requirements to FAE server.

   1b. FAE server receives from the FF application specific server a request to adapt the application requirements. This request can comprise the change of service profile/requirements mapped to app#A.

2. FAE server determines the re-mapping of app#A to slice #2. This mapping is based on the updated application requirements (as of step 1a or 1b), the per UE slice subscriptions (for all UEs running app#A), slice capabilities and availability and the GST parameters.

3. FAE server sends the updated app to slice mapping to the SEAL Server (e.g. NRx server). This message indicates the requirement for mapping the application traffic from slice #1 to slice #2.

4. The SEAL Server, acting as AF, sends a Nnef_service_parameter create or update request to NEF (as provided in TS23.502 [12] clause 4.15.6.7). The Service Description can be represented by the application identifier (App#A ID) and a combination of the DNN and the target S-NSSAI (slice #2). The updated Service Description is stored in the UDR. The UDR then notifies the PCF and the PCF provides the updated UE policies to the affected UEs.

5. The SEAL server sends a Notification to the FAE server on the completion of the re-mapping of App#A to slice #2.

Editor's note: The enhancement of SEAL (e.g. NRx) to process the slice re-mapping instruction and generate an AF request to trigger the slice re-mapping towards 5GS as described in steps 1-3 is FFS.

Editor's note: Potential overlaps with SA2 for this solution are FFS.

7.13.2 Solution evaluation

This is an alternative technical solution for the FF application-triggered network slice re-mapping by enhancement of SEAL, it may overlap with SA2 or functionality might be missing there. SA2 should be contacted before proceeding with normative work.

7.14 Solution #14 clock synchronization

7.14.1 General

This solution addresses the key issue 3: clock synchronization.

7.14.2 Solution description

As specified in clause 5.27 of TS 23.501[7], the mechanisms for TSN time synchronization is designed.

For TSN time synchronization, the entire E2E 5G system can be considered as an IEEE 802.1AS [5] "time-aware system". Only the TSN Translators (TTs) at the edges of the 5G system need to support the IEEE 802.1AS [5] operations. UE, gNB, UPF, NW-TT and DS-TTs are synchronized with the 5G GM (i.e. the 5G internal system clock) which shall serve to keep these network elements synchronized. The TTs located at the edge of 5G system fulfil all functions related to IEEE 802.1AS [5], e.g. (g)PTP support, timestamping, Best Master Clock Algorithm (BMCA), rateRatio.

The TSN time synchronization is addressed by the TSN translators, which is in SA2 scope.

7.14.3 Solution evaluation

This solution uses TSN time synchronization mechanisms specified in clause 5.27 of Rel-16 3GPP TS 23.501[7], it is in SA2 scope, no need normative work.

7.15 Solution 15: Time Synchronization Management

7.15.1 Time Synchronization support

SA2 FS_IIOT study in 3GPP TR 23.700-20 [13] contains solutions addressing the exposure of Time Synchronization capabilities by NEF. Exposed Time Synchronization capabilities include:

- Support for Time Synchronization.

- Supported time synchronization methods.
- Supported (g)PTP versions.
- Minimum Time Synchronization accuracy supported.
- Minimum gPTP or PTP message generation supported.
- Maximum number of clients that can be supported at the minimum gPTP or PTP message rate.

3GPP TR 23.700-20 [13] has introduced procedures to expose 5G time synchronization information to aid the AF/FAE server to use Time Synchronization in 5GS. Based on this and in order to support time synchronization to FF specific applications, it is proposed that the SEAL Network Resource Management (NRM) server exposes the Time synchronization capabilities obtained from NEF via N33 to Application Specific Servers that need to use the Time Synchronization Service.

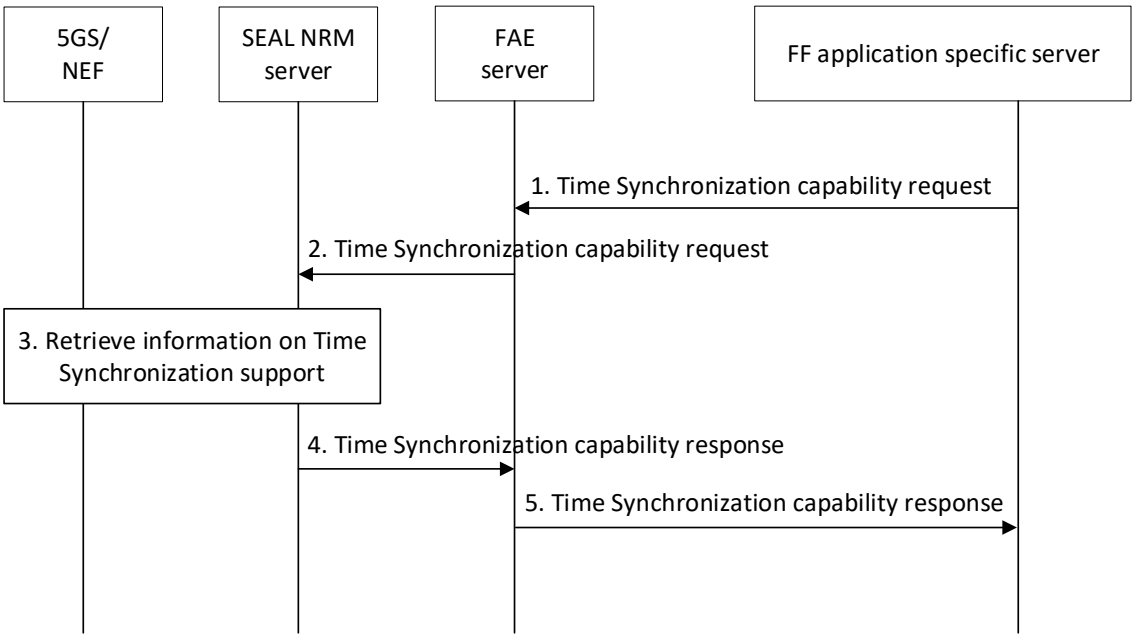

Figure 7.15.1-1: Procedure to request time synchronization capabilities

1. The FF application specific server sends a Time Synchronization capability request to the FAE server in order to learn about the supported time synchronization capabilities.
2. The FAE server forwards the request to the SEAL NRM server.
3. The SEAL NRM server authorizes the request and interacts with the 5GS/NEF server to retrieve the time synchronization capability information. The SEAL NRM server may cache this information to satisfy future requests.
4. The SEAL NRM server sends a response to the FAE server with the information about the supported time synchronization capabilities if step 3 was successful. Otherwise it sends a failure response.
5. The FAE server forwards the response to the FF application specific server.

7.15.2 Time Synchronization activation/deactivation/modification

3GPP TR 23.700-20 [13] has also introduced solutions addressing Time Synchronization services. These services can be used by an AF to request time synchronization with specified requirements, and supply information that can be used to optimize and configure time synchronization procedures for connected devices. These solutions include procedures for an AF to request Time Synchronization in 5GS for a UE or a group of UEs, such as time synchronization method, (g)PTP versions, Timing Domain, grandmaster priorities, required synchronization accuracy.

Assuming that the information about supported time synchronization capabilities has been provided to the FF application specific server, as described in clause 7.15.1, it is proposed that the SEAL NRM server is further enhanced

to offer Time Synchronization activation/deactivation/modification services to the FF Application Enabler (FAE) Server using 5GS services via NEF. For that, SEAL NRM server sends a Time Sync Service Request to the NEF indicating the target UE(s) and the clock domain to activate/deactivate/modify UE's time synchronization service.

Editor's note: How time synchronization could be supported in the FAE layer when not supported by 5GS is FFS.

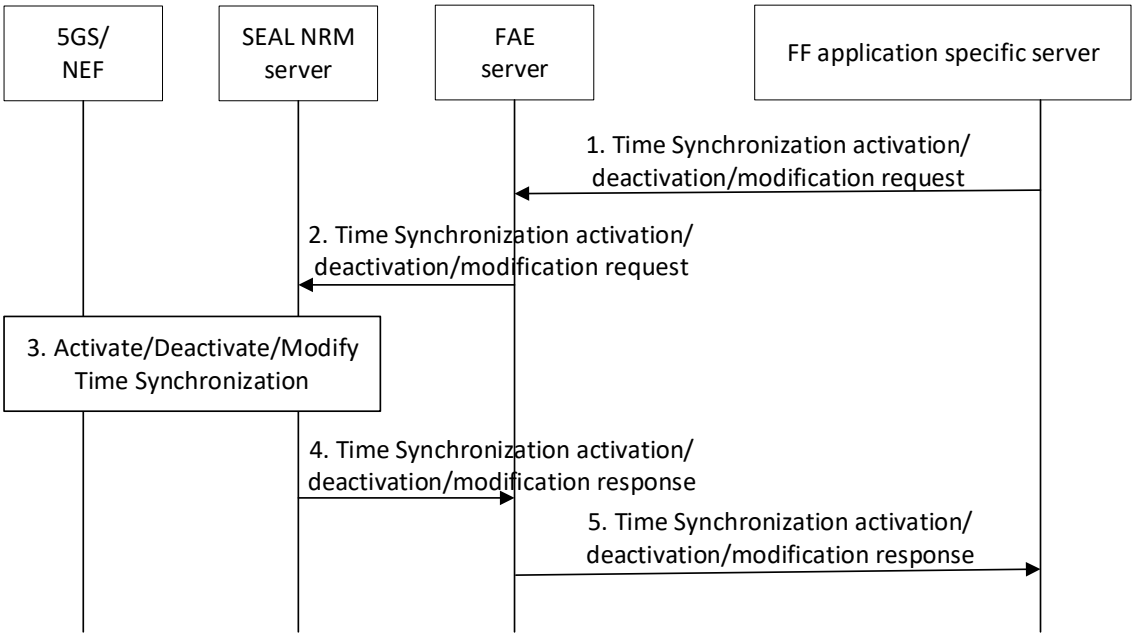

Figure 7.15.2-1: Procedure to activate/deactivate/modify time synchronization

1. The FF application specific server sends a Time Synchronization activation/deactivation/modification request to the FAE server with a list of VAL UEs and/or a VAL group ID that are the target of the request and the clock domain when applicable.
2. The FAE server forwards the request to the SEAL NRM server.
3. The SEAL NRM server authorizes the request and interacts with the 5GS/NEF server to activate/deactivate/modify the time synchronization service for the target UEs.
4. The SEAL NRM server sends a response to the FAE server with the result of step 3. If step 3 was successful the SEAL NRM server sends a success response, otherwise it sends a failure response.
5. The FAE server forwards the response to the FF application specific server.

7.15.3 Solution evaluation

This solution depends on SA2 addressing requirements regarding the exposure of time synchronization via NEF. 3GPP TR 23.700-20 [13] has already started to address solutions to provide generic mechanisms for exposure of time synchronization services via NEF. The specification of such mechanisms, therefore, will be required to be used as the baseline when the solution described in this clause is addressed during the normative work.

7.16 Solution #16: TSN policy negotiation via FAE layer

7.16.1 Solution description

This solution function addresses the Key issue #4 for enabling the negotation via the FAE layer of the TSN application QoS requirements (e.g. survival time) and their mapping to network policies / QoS parameters.

7.16.1.1 General

This solution takes as input a trigger event based on the monitored QoS parameters (by SEAL / NRx or by the network) and based on this, it generates a trigger which may be in the form of a proposed action, which can be a policy related to the 1) adaptation of application requirements (e.g. survival time, TSC service area, mobility change) or 2) adaptation of port management policies (DS-TT, NW-TT policies). TSN system (FF application specific server which is equivalent to CNC) may then provide a request for adaptation of the configuration based on these requirements, and FAE server will send these policies to the corresponding Devices (FAE clients).

An example for TSN policy negotiation corresponding to port management policies and service requirements is when high jitter is monitored for an ongoing session, the hold & forward buffering parameters may be adapted to de-jitter the TSC flows. However, this will have impact on the survival time, since the delayed reception of the traffic, may lead to service termination (due to reaching the survival time threshold). In this case, FAE server interacts with the CNC for triggering the adaptation of the survival time/ tolerance to loss value, in combination with the hold & forward buffering parameters.

7.16.1.2 Procedure

Pre-condition 1: UE is registered to 5GS and FAE client has established a connection with FAE server.

Pre-condition 2: FF application specific server has subscribed to FAE server to receive TSN related triggers.

Pre-condition 3: FAE server has subscribed to the SEAL server / NRx (based on Solution #10 of TR 23.745) or to the PLMN (e.g. QoS monitoring for URLLC as specified in clause 5.33.3 of TS 23.501 [7]) for receiving QoS events.

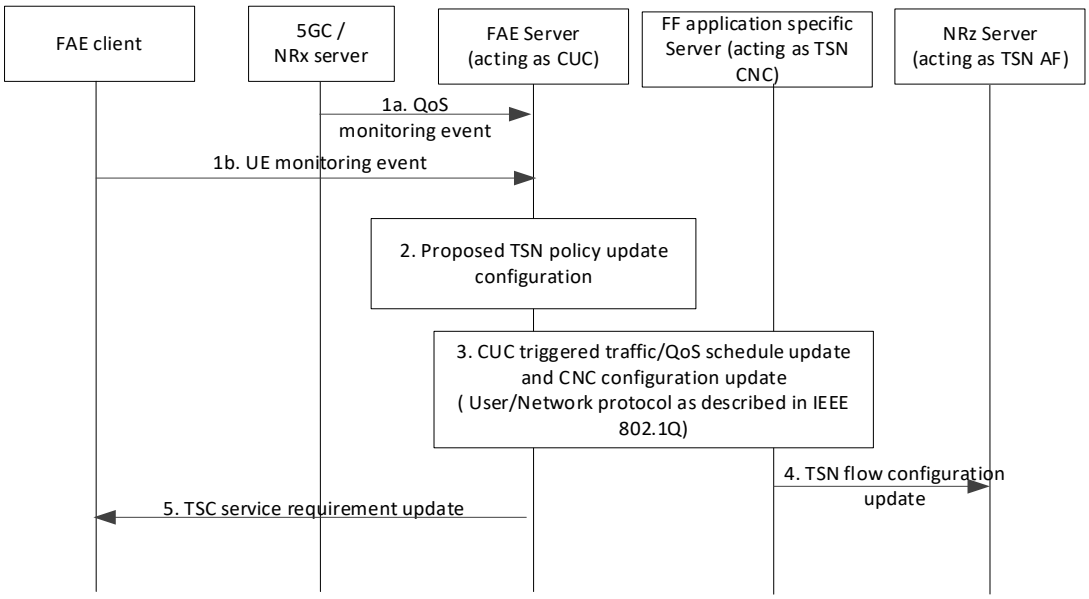

Figure 7.16.1.2-1: TSN Policy update negotiation

1a. A QoS monitoring event is sent from either SEAL/NRx (based on Solution #10 of TR 23.745) or PLMN/NEF to the FAE server based on the subscription (e.g. event related to high jitter for TSC flow).

1b. Alternatively to 1a, a UE related monitoring event, which may relate to a UE related event (e.g. change of UE or group mobility/speed, inter-UE distance change, location reporting) or an application-related event (notification that maximum survival time is reached for the TSC service, high jitter, etc).

2. FAE server upon receiving the QoS and/or UE-related monitoring event for one or more TSC flows, determines a trigger, which can be a proposed TSN policy update for all or subsets of the TSC flows within the FF application. The trigger may take the form of a new service requirement, QoS requirement or network requirement for the TSC flows, taking also into account the location of the UEs (which can be provided by LM server).

3. The FAE server, acting as CUC, sends an abstracted report, enclosing a notification on an experienced/expected change of application requirement /application QoS metric based on the received event to FF application specific

server / CNC. CNC may adapt the configuration, and then sends a TSN policy update to FAE server, including the new policy parameters based on the proposed policy parameters. The new policy update may take the form of a new QoS/network/service requirement for the TSC flows of the end devices. This exchanged is performed via User/Network protocol as being specified in IEEE 802.1Qcc [25].

4. The FF application specific server sends a TSN flow configuration update to the NRz server (NRz server, acting as TSN AF, receives from FF application specific server, acting as CNC, policy parameters and related flow information according to IEEE 802.1Q [6]), if the TSN policy update relates to the update of the QoS policies for the TSN flows. If the TSN policy update relates to NW-TT/DS-TT port management policy update, NRz interacts with NW-TT and DS-TT to apply the new policy (TSN AF to NW-TT/ DW-TT transfer of port or bridge management information, as defined in TS23.501 [7], clause 5.28.3.2). NRz server has been defined in Solution #22 of TR23.745.

5. The FAE server sends a service requirement update message to the involved FAE clients. This message includes the agreed policy update type and parameters. Then, further interaction with FF application specific client is needed for applying the new parameters (e.g. survival time increase).

Editor's note: In this solution, the transformed information may take the form of a proposal of a TSN policy / requirements update for the respective FF application. However, it is FFS what transformed information is needed for supporting such update.

7.16.2 Solution evaluation

This solution provides a mechanism, involving the FAE, for transforming a monitoring event from the network or UE side, to an abstracted report which can be used by FF application specific server to adapt the TSN policies for one or more devices running TSC services. This solution provides an enhancement for pro-actively alerting the CNC on expected performance downgrade, while minimizing the complexity/overhead at the FF application specific server (for processing all related network/UE triggered monitoring events). TSN-based ecosystems are configured to explicitly support the required QoS at the application layer. This solution provides a mechanism to enable the application layer to make adjustments when QoS conditions occur that affect the ability for the application to function normally; however it is still unclear in which use cases such QoS abnormalities can be accommodated for in TSN networks. This solution will be considered for normative work if a valid use case is identified where this solution provides value.

Editor's note: Whether the FAE server can act as CUC is FFS.

7.17 Solution #17: Support TSN in FF Application Enabler layer

7.17.1 Solution description

This solution is only support TSN in FF Application Enabler (FAE) layer, not include SEAL services.

Figure 7.17.1-1 illustrates the FF function model to support TSN in FAE layer.

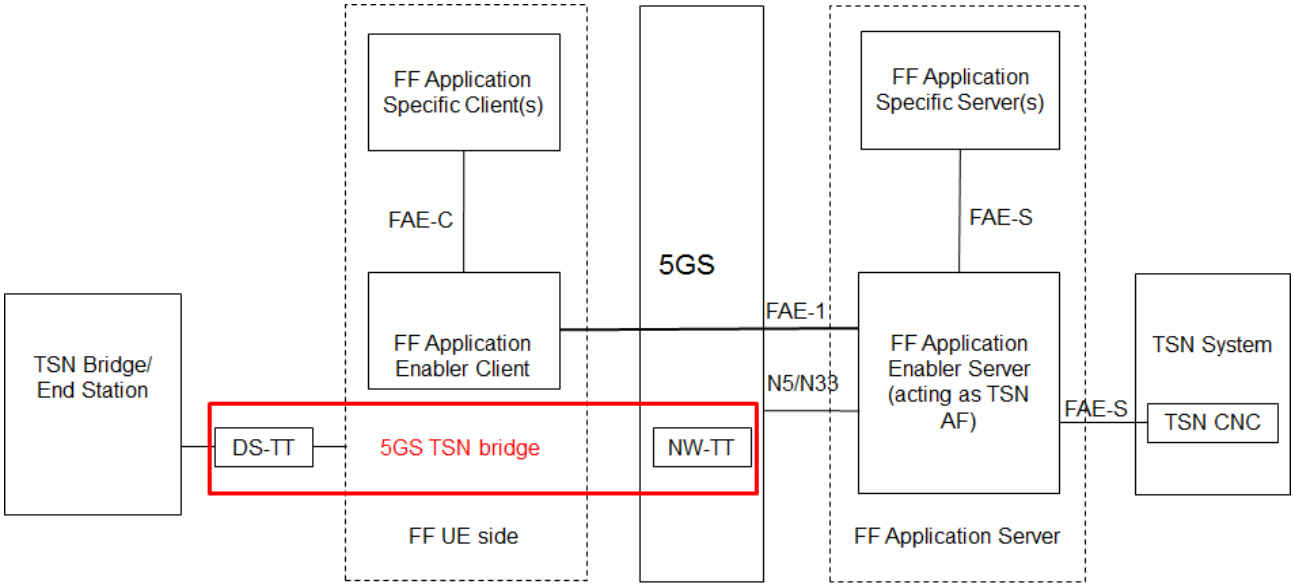

Figure 7.17.1-1: Functional model to support TSN in FAE layer

According to clause 4.4.8 Time Sensitive Communication and clause 5.28 Support of integration with TSN specified in 3GPP TS 23.501 [7], in order to support TSN in application layer, the FF UE interacts with DS-TT, the FAE server acting as TSN-AF and links to TSN CNC over FAE-S reference point following IEEE 802.1Qcc [25]. The FAE server acting as TSN AF manages the 5GS TSN bridge (including DS-TT and NW-TT) through N5/N33 reference point specified in 3GPP TS 23.501[7]. The FF application specific client provides the client side functionalities corresponding to the TSN applications (e.g. motion control, control-to-control communication, mobile robots, mobile control panels). The FF application specific server provides the server side functionalities corresponding to the TSN applications.

Editor's Note 1: The FAE client can also be outside of the UE.

Editor's Note 2: Reuse of the TSN channel by the FAE layer (e.g.FAE-1) is FFS.

7.17.2 Solution evaluation

This solution supports FAE server acting as TSN AF without SEAL, which depends TSC capabilities already specified on Rel-16 3GPP TS 23.501 [7] and solutions currently studied in 3GPP TR 23.700-20 [13].

7.18 Solution #18: Device monitoring

7.18.1 Solution description

7.18.1.1 General

This solution corresponds to the Key issue #14 - Device monitoring.

3GPP TS 23.501 [7] defines NEF to support external exposure of capabilities of network functions. Monitoring capability can be used for exposing UE's mobility management context such as UE location, reachability, roaming status, and loss of connectivity.

3GPP TS 29.522 [11] & 3GPP TS 29.122 [26] defines MonitoringEvent API for exposure of monitoring capability, including detail monitoring events (e.g. LOSS_OF_CONNECTIVITY, UE_REACHABILITY, LOCATION_REPORTING, ROAMING_STATUS, COMMUNICATION_FAILURE, Availability_after_DDN_failure_notification_enhancement, PDN_CONNECTIVITY_STATUS, Downlink_data_delivery_status_5G, etc.) for device monitoring.

Expose monitoring capability is a common functionality for all verticals (and not only V2X and FF), so SEAL should to enhance to support.

The FAE server can utilize Network Resource Management of SEAL to support device monitoring. Which needs to enhance the existing Network Resource Management service enabler by invoking MonitoringEvent API through NEF defined in 3GPP TS 29.522 [11] & 3GPP TS 29.122 [26].

7.18.1.2 Device monitoring procedure

The procedure for device monitoring is illustrated in figure 7.18.1.2-1.

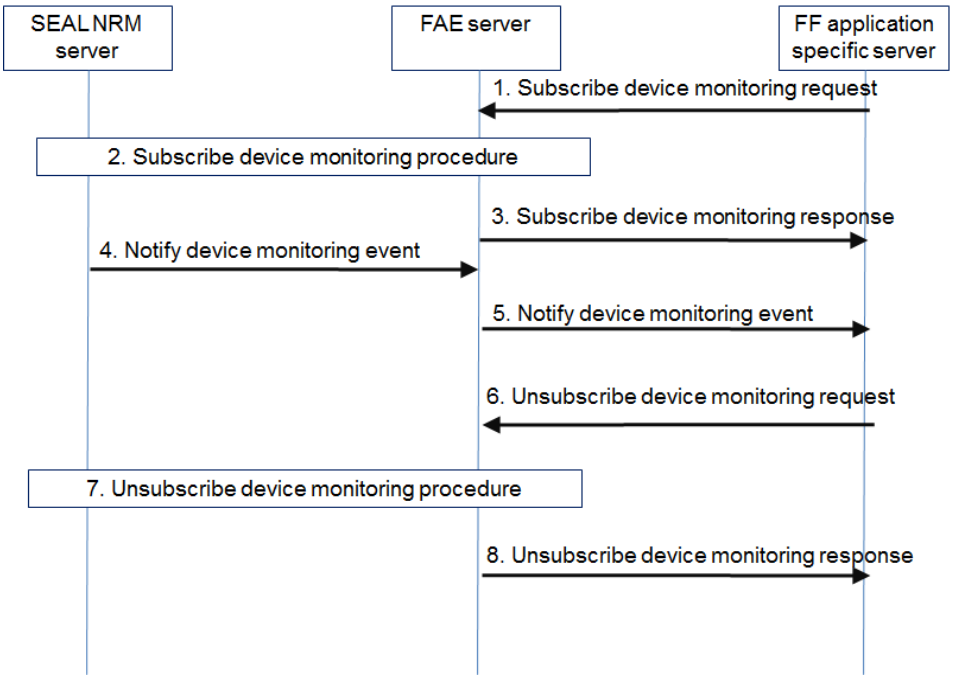

Figure 7.18.1.2-1: Device monitoring procedures

1. The FF application specific server sends a device monitoring subscribe request (which include monitor event types, e.g. UE location, reachability, roaming status, and loss of connectivity, etc.) to the FAE server. The FF application specific server don't need to have knowledge of 5G network events, just monitor event types. The FAE server exposes the monitor event types to FF application specific server, those higher abstraction are based on SEAL NRM server providing a higher abstraction level of the NEF monitoring events to the FAE server.

2. The FAE server determines device or group information which based on criterias such as location area. Then the FAE server forwards the request to SEAL NRM server to subscribe to device monitoring events. The SEAL NRM server interacts with the NEF to establish a device monitoring subscription (not shown in the sequence). In that interaction the SEAL NRM server determines device monitoring events (e.g. LOSS_OF_CONNECTIVITY, UE_REACHABILITY, LOCATION_REPORTING, ROAMING_STATUS, COMMUNICATION_FAILURE, Availability_after_DDN_failure_notification_enhancement, PDN_CONNECTIVITY_STATUS, Downlink_data_delivery_status_5G, etc.). The SEAL NRM server could provide further operations, e.g. offering different monitoring levels, maping to subsets of the NEF events, caching events, mapping of identities, etc.

3. The FAE server sends a device monitoring subscribe response to the FF application specific server.

4. When device monitoring event is triggered and the SEAL NRM server is notified by the NEF (not shown in the sequence), the SEAL NRM server matches the criteria for the subscribed device monitoring type and generates the higher abstraction level event, then sends a device monitoring notification to the FAE server.

5. The FAE server notifies the FF application specific server about the device monitoring event.

NOTE: Steps 4 and 5 are repeated when device monitoring events occur.

6. When the FF application specific server decides to unsubscribe for the device monitoring, the FF application specific server sends a device monitoring unsubscribe request to the FAE server.

7. The FAE interacts with the SEAL NRM server to unsubscribe from device monitoring events. The SEAL NRM server interacts with the NEF to terminate the device monitoring subscription (not shown in the sequence).

8. The FAE server sends a device monitoring unsubscribe response to the FF application specific server.

Editor's Note: It is FFS to clarify the functionality of FAE server for device monitoring.

7.18.2 Solution evaluation

This solution depends on how SEAL to support NEF MonitoringEvent API. The specification of such a mechanism, therefore, will be required to be used as the baseline when the solution described in this clause is addressed during the normative work.

7.19 Solution #19: Communicating FF application service requirements with 3GPP system

7.19.1 Solution description

This solution corresponds to the key issue #8 on communication of FF application requirements with 5GS and key issue#11 on QoS coordination. The procedure for communicating FF application service requirements from FF application specific server utilizes the procedures specified in clause 14.3.4 of 3GPP TS 23.434 [8]. The NRM server is to be enhanced to additionally support translating the FF application service requirements to 3GPP network requirements.

7.19.2 Solution evaluation

This is a viable technical solution for key issue#8. The NRM server acts a generic server which may be co-located with FF application specific server and may be capable to translate the FF application specific requirements to 3GPP transport specific requirements.

7.20 Solution #20: SEAL support for CoAP to address constrained devices

7.20.1 Solution description

7.20.1.1 Introduction

This solution addresses key issue 16 – Constrained devices - with regards to the architectural SEAL enhancements needed to address such devices.

The purpose of SEAL is to provide generic service enablers to address requirements common to various vertical applications. SEAL defines a generic architecture, service enablers, protocols, and APIs in 3GPP TS 23.434 [8] in stage 2 and a set of stage 3 specifications.

As described in 3GPP TS 23.434 [8], SEAL-UU is a generic reference point for interactions between a SEAL client and a corresponding SEAL server. Each SEAL service specifies its SEAL-UU reference point and the protocol(s) used in that reference point. The present SEAL services make a choice of using HTTP and/or SIP in the SEAL-UU reference point. Clause 6.2 of 3GPP TS 23.434 [8] specifies the functional model of the SEAL signalling control plane, which is based on SIP and HTTP. While these protocols are well established and performant for non-constrained devices, they are problematic for battery-driven, CPU and memory constrained devices.

The Constrained Application Protocol (CoAP) is a protocol defined by IETF in RFC 7252 [27] and designed specifically for application layer communication for constrained devices. CoAP provides a request/response interaction model between application endpoints, supports built-in discovery of services and resources, and includes key concepts of the Web such as URIs and Internet media types. CoAP is designed to easily interface with HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead, and simplicity for constrained environments. RFC 7252 [27] specifies bindings to UDP and DTLS. IETF RFC 8323 [28] specifies bindings to TCP, WebSocket and TLS.

CoAP has the following main features:

- Web protocol fulfilling requirements in constrained environments, realizing the REST architecture
- Unreliable transport with UDP binding with optional reliability supporting unicast and multicast requests, and security binding to DTLS
- Reliable transport with TCP and WebSocket binding, and security binding to TLS
- Asynchronous message exchanges
- Low header overhead and parsing complexity
- URI and Content-type support
- Simple proxy and caching capabilities
- A stateless HTTP mapping, allowing proxies to be built providing access to CoAP resources via HTTP in a uniform way or for HTTP simple interfaces to be realized alternatively over CoAP

This solution proposes to introduce CoAP as an additional protocol for the SEAL signalling control plane. The following IETF documents are considered relevant for this purpose, and are listed here for reference:

a) The Constrained Application Protocol (CoAP) – RFC 7252 [27]. It defines the CoAP protocol, messaging model, format, request/response semantics as well as options and other header parameters.

b) CoAP over TCP, TLS, and WebSockets – RFC 8323 [28]. It outlines the changes required to use CoAP over TCP, TLS, and WebSockets transports. The primary reason for introducing CoAP over TCP and TLS is that some networks do not forward UDP packets. Additionally, Where NATs are present along the communication path, CoAP over TCP leads to different NAT traversal behavior than CoAP over UDP.

c) Block-Wise Transfers in CoAP – RFC 7959 [29]. It defines blockwise transfers over CoAP, for large payloads.

d) Observing Resources in CoAP – RFC 7641 [30]. It specifies a simple protocol extension for CoAP that enables CoAP clients to "observe" resources, i.e., to retrieve a representation of a resource and keep this representation updated by the server over a period of time.

e) Constrained RESTful Environments (CoRE) Link Format – RFC 6690 [31]. It defines Web Linking using a link format for use by constrained servers to describe hosted resources, their attributes, and other relationships between links.

f) Object Security for Constrained RESTful Environments (OSCORE) – RFC 8613 [32]. It provides end-to-end protection between endpoints communicating using CoAP or CoAP-mappable HTTP.

g) Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth - draft-ietf-ace-oauth-authz-35 [33]. It describes a framework for authentication and authorization in constrained environments built on re-use of OAuth 2.0, thereby extending authorization to IoT devices.

7.20.2 SEAL functional model for signalling control plane including CoAP

Clause 6.2 in TS 23.434 [8] shows SEAL functional model for the signalling control plane. CoAP-based entities and reference points are introduced to the functional model, as shown in the figure 7.20.2-1.

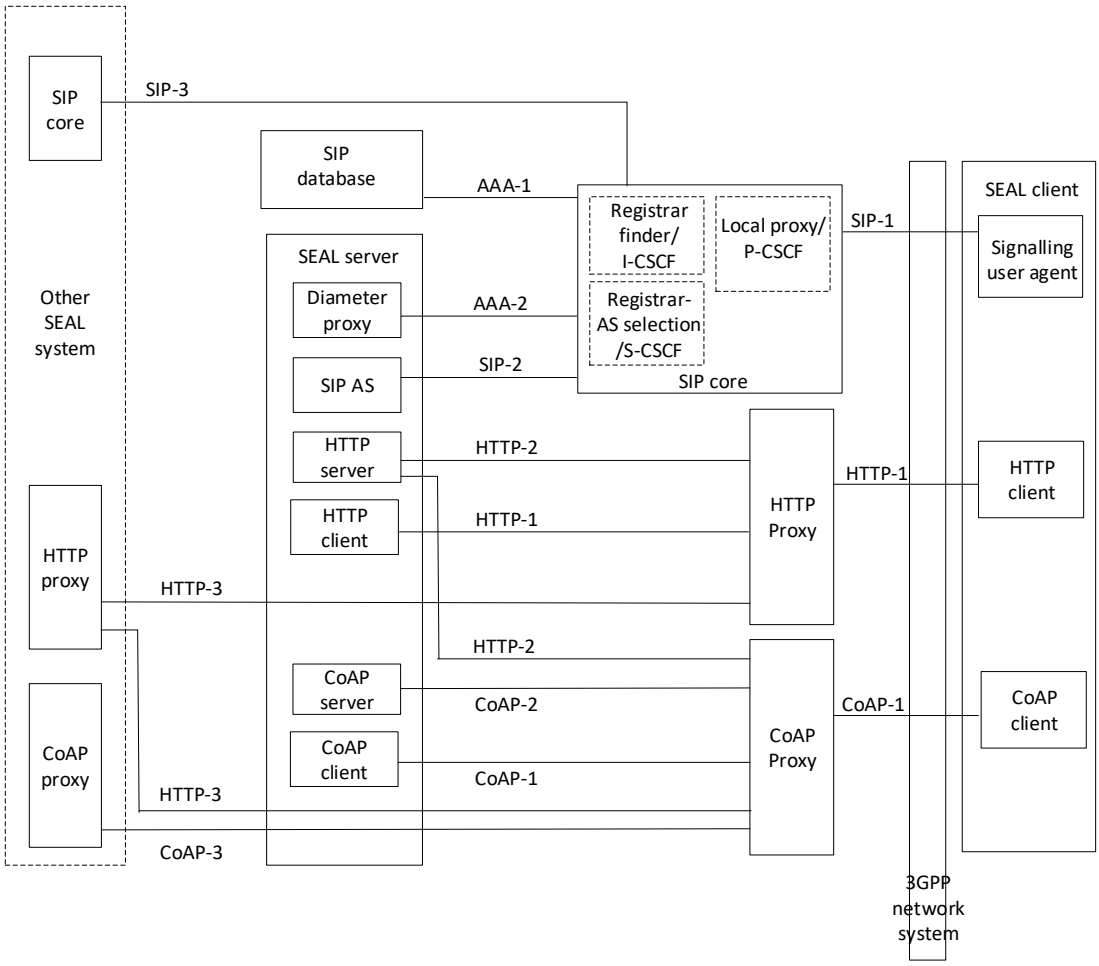

Figure 7.20.2-1: SEAL functional model for signalling control plane including CoAP entities

The proposed CoAP signalling entities and reference points are described further in clauses 7.20.3 and 7.20.4, respectively.

7.20.3 CoAP entities

7.20.3.1 CoAP client

This functional entity acts as the client for all transactions of the SEAL client executing in a constrained UE. An unconstrained UE may choose to use the CoAP client if it is available.

7.20.3.2 CoAP proxy

This functional entity acts as a proxy for transactions between the CoAP client and one or more CoAP servers. The CoAP proxy terminates a DTLS, TLS or secure WebSocket session on CoAP-1 reference point with the CoAP client of the VAL UE allowing the CoAP client to establish a single secure session for transactions with multiple CoAP servers that are reachable by the CoAP proxy.

CoAP proxy can act as a cross-protocol CoAP-HTTP proxy to enable CoAP clients to access resources on HTTP servers on HTTP-2 reference point.

The CoAP proxy terminates CoAP-3 reference point that lies between different CoAP proxies. It may provide a topology hiding function from CoAP entities outside the trust domain of the VAL system.

The CoAP proxy can also terminate HTTP-3 reference point for interworking with another HTTP proxy. In this role it provides cross-protocol mapping and may provide a topology hiding function from HTTP entities outside the trust domain of the VAL system.

The CoAP proxy shall be in the same trust domain as the CoAP clients and CoAP servers that are located within a VAL service provider's network. There can be multiple instances of a CoAP proxy e.g. one per trust domain.

NOTE: The number of instances of the CoAP proxy is deployment specific.

7.20.3.3 CoAP server

This functional entity acts as the CoAP server for all CoAP transactions of the SEAL server.

7.20.4 Signalling control plane reference points for CoAP

7.20.4.1 Reference point CoAP-1 (between the CoAP client and the CoAP proxy)

The CoAP-1 reference point exists between the CoAP client and the CoAP proxy. The CoAP-1 reference point is based on CoAP (which may be secured using DTLS when run on UDP or TLS when run on TCP or WebSocket).

7.20.4.2 Reference point CoAP-2 (between the CoAP proxy and the CoAP server)

The CoAP-2 reference point, which exists between the CoAP proxy and the CoAP server, is based on CoAP (which may be secured using DTLS when run on UDP or TLS when run on TLS).

7.20.4.3 Reference point CoAP-3 (between the CoAP proxy and CoAP proxy)

The CoAP-3 reference point, which exists between the CoAP proxy and another CoAP proxy in a different network, is based on CoAP (which may be secured using DTLS when run on UDP or TLS when run on TLS).

7.20.5 CoAP usage

CoAP is introduced as an optional protocol to be used by the SEAL service enablers on their respective SEAL-UU reference points, e.g. key management, location management, group management, configuration management and identity management. A SEAL client serving a constrained device should use the CoAP-1 reference point with the CoAP proxy and may use either the CoAP-2 or the HTTP-2 reference point for transport and routing of the related signalling with the SEAL server.

CoAP may be used for interactions between SEAL servers on their respective SEAL-X reference points. For this usage a SEAL-X reference point shall use the CoAP-1 and either the CoAP-2 or the CoAP-3 reference point depending on the trust relationship between the interacting SEAL servers.

7.20.6 Solution evaluation

This solution provides enhancements to the SEAL functional model for the signalling control plane by adding support of CoAP to address constrained devices. This solution addresses the gaps described in key issue #16.

7.21 Solution #21: Enabling 5G CN capabilities for SEAL Groups

7.21.1 Solution description

This solution corresponds to the Key issue #17 – Using 5G CN capabilities for SEAL Groups. The solution proposes that the SEAL server obtains the external group identifier for a group of UEs, from the core network and includes it the SEAL group document at the time of group creation. This provides a mapping of the SEAL group to a core network known external group identifier, which can then be be used by the SEAL servers or the FF application layer servers for invoking any SCEF/NEF APIs related to the SEAL group.

SEAL GMS then stores this external group identifier within the SEAL group document. Further, any SEAL server or the FF application server can fetch the external group identifier from the SEAL GMS using the VAL Group ID and use it for any NEF/SCEF invocations like monitoring APIs for UE reachability, location etc.

This solution is also applicable for other verticals like UASAPP, V2XAPP etc, where SEAL or VAL has to to invoke SCEF/NEF APIs related to the group of UEs to fufill the vertical specific requirements.

7.21.2 SEAL Group creation procedures

The external group identifier (as specified in 3GPP TS 23.682 [34]), identifying the group of UEs, is stored in the newly created VAL group document at the time of SEAL group creation. This clause illustrates how external group identifier is assigned to VAL group document during various SEAL creation procedures as specified in 3GPP TS 23.434 [8].

As shown in Figure 7.21.2-1, during the SEAL group creation procedure as specified in clause 10.3.3 of 3GPP TS 23.434 [8], in step 3, the SEAL GMS server uses the external group identifier identifying the member UEs in the VAL group and stores the external group identifier in the newly created VAL group document.

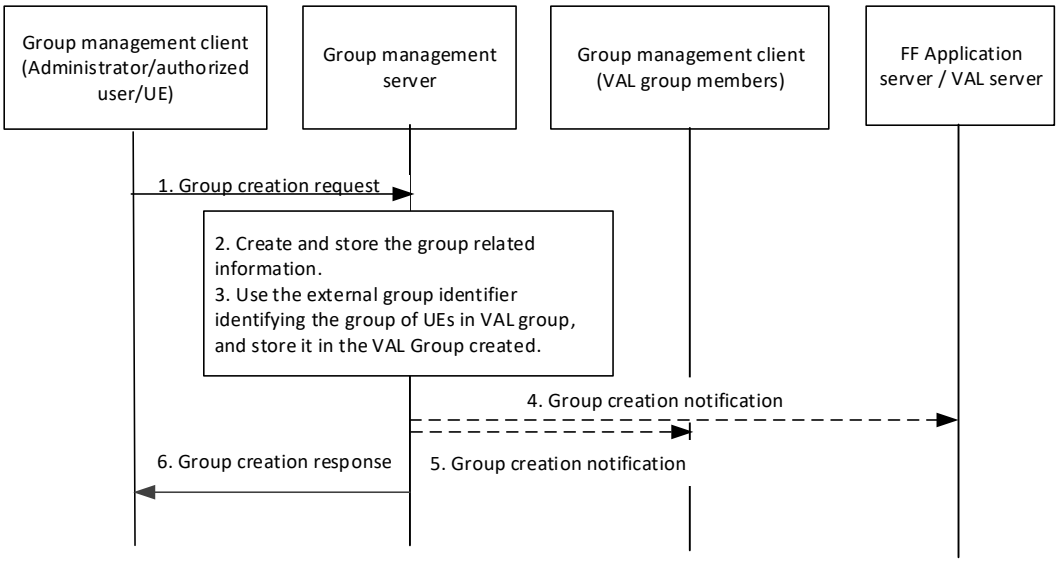

Figure 7.21.2-1: SEAL group creation

As shown in Figure 7.21.2-2, during the location based SEAL group creation procedure as specified in clause 10.3.7 of 3GPP TS 23.434 [8], in step 6, the SEAL GMS server uses the external group identifier for the list of UEs obtained from Location Management Server in step 4 and store the external group identifier to the newly created VAL group document.

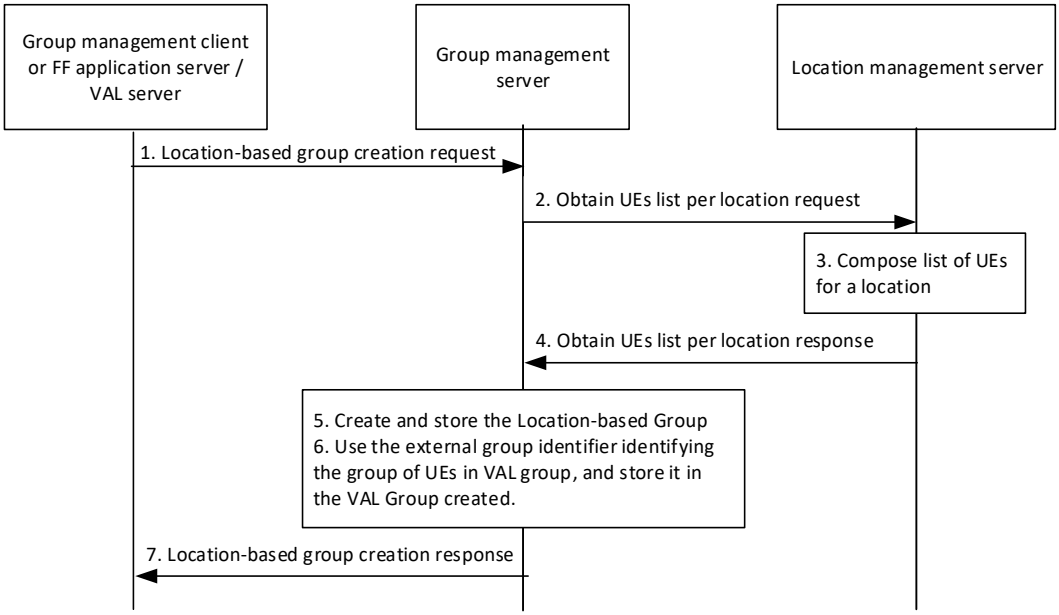

Figure 7.21.2-2: Location-based SEAL group creation

As shown in Figure 7.21.2-3, during the group announcement and join procedure as specified in clause 10.3.8 of 3GPP TS 23.434 [8], in step 4, the SEAL GMS server uses the external group identifier for the list of UEs and stores the external group identifier in the newly VAL group document.

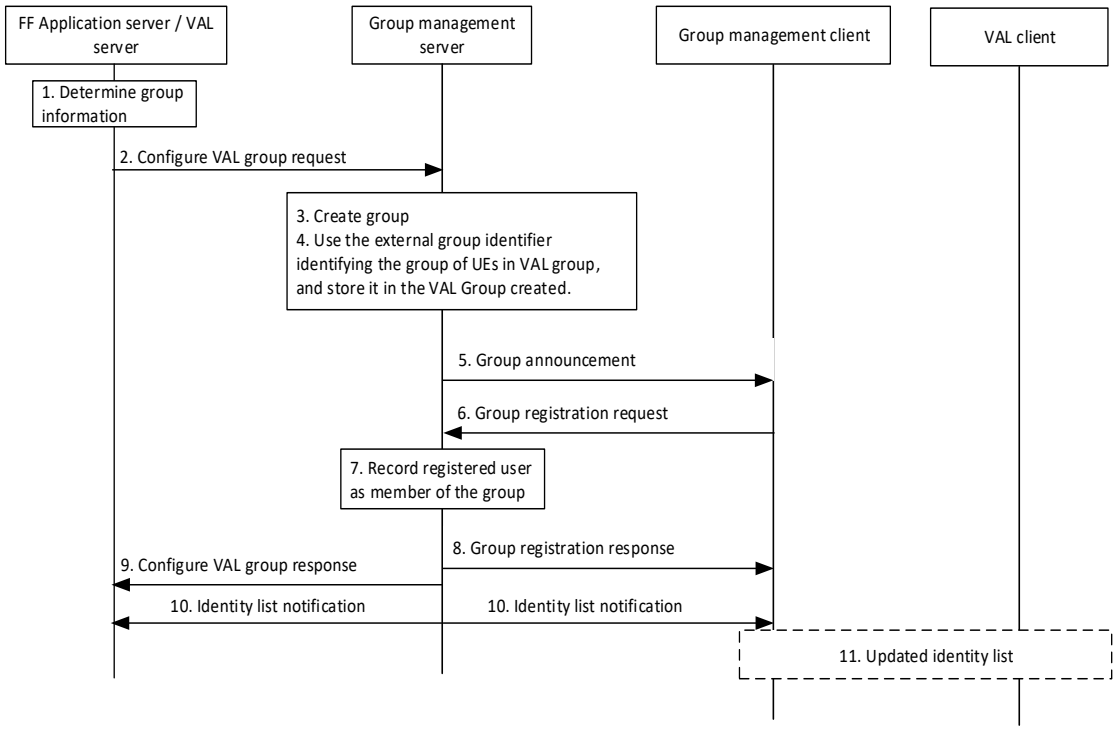

Figure 7.21.2-3: Group announcement and join procedure

For group management procedures pertaining to a 5GLAN group, to create or modify the external group identifiers, the SEAL group management server will use dynamic 5G VN group management procedures exposed by NEF via the N33 reference point (as specified in TS 23.501 [7] and TS 23.502 [12]).

Note: For SEAL groups not pertaining to 5GLAN group, management of the external group identifier may require alignment with SA2 work in future.

7.21.3 Solution evaluation

This solution provides enhancements to SEAL GMS supporting the external group identifier (identifying a group of UEs by the 3GPP CN) in SEAL Group Management procedures. This enables the SEAL and FFAPP layer servers to invoke the SCEF/NEF APIs for the member UEs of the VAL group using the external group identifier managed by the 3GPP CN. This solution addressess the gaps described in Key Issue #17.

7.22 Solution #22: SEAL support for TSC services

7.22.1 Introduction

This solution addresses architectural aspects related to Key Issue #4 on TSN support, Key Issue #11 on QoS coordination, and Key Issue #8 on communication of FF application requirements.

This contribution proposes an architecture to expose Time Sensitive Communication (TSC) capabilities of the 5G system which supports integration with an IEEE TSN system as well as 5G-native (i.e. non-TSN) TSC services. Due to the common nature of these TSC capabilities (which can be used by various verticals), it is proposed to enhance the SEAL Network Resource Management service enabler by adding support for TSC capabilities.

The SEAL NRM service enabler will make use of the 5GS TSC capabilities available via the N5 reference point.

In the Rel-16 specification 3GPP TS 23.501 [7] 5GS supports integration with IEEE 802.1 TSN networks applicable for the fully centralized configuration model as defined in IEEE Std 802.1Qcc [25]. In that model the Centralized Network Configuration (CNC) server sets up the TSN flows across the 5GS virtual bridges based on the TSN stream requests from CUC and the 5GS virtual bridge capabilities provided by the TSN AF.

For the case of TSN integration, this solution proposes that the NRM server will act as a TSN AF and will interact with the CNC via the NRM-S reference point using the IEEE 802.1Qcc [25] management protocol. The NRM server will interact with the 5GC via N5 reference point as specified in 3GPP TS 23.501 [7].

For the case of 5G-native TSC services, this solution proposes that the NRM server will support management of the end-to-end QoS flows in the 5GS. This will enable an FF application to request configuration of TSC QoS flows between UEs within the 5GS via the NRM-S reference point. The NRM server will perform QoS coordination for the set of UEs and their respective QoS flows referred-to in KI#11. In this case the NRM-S reference point will specify a 3GPP protocol for this interaction. The NRM server will also configure the NRM clients with the TSC parameters for their QoS flows. The NRM server will interact with the 5GC via N5 reference point as specified in 3GPP TS 23.501 [7].

7.22.2 Solution description

The architecture for integration of the 5G with TSN is depicted in Figure 7.22.2-1. The SEAL NRM server acts as a TSN AF. Upon request from an FF Application layer server acting as a TSN CNC via the NRM-S reference point it configures the TSN flows in the 5GS. In this case the NRM-S supports the IEEE 802.1Qcc management protocol. As a TSN AF the SEAL NRM server interacts with the 5GS PCF over the N5 reference point to configure the 5G QoS and TSCAI parameters in the 5GS.

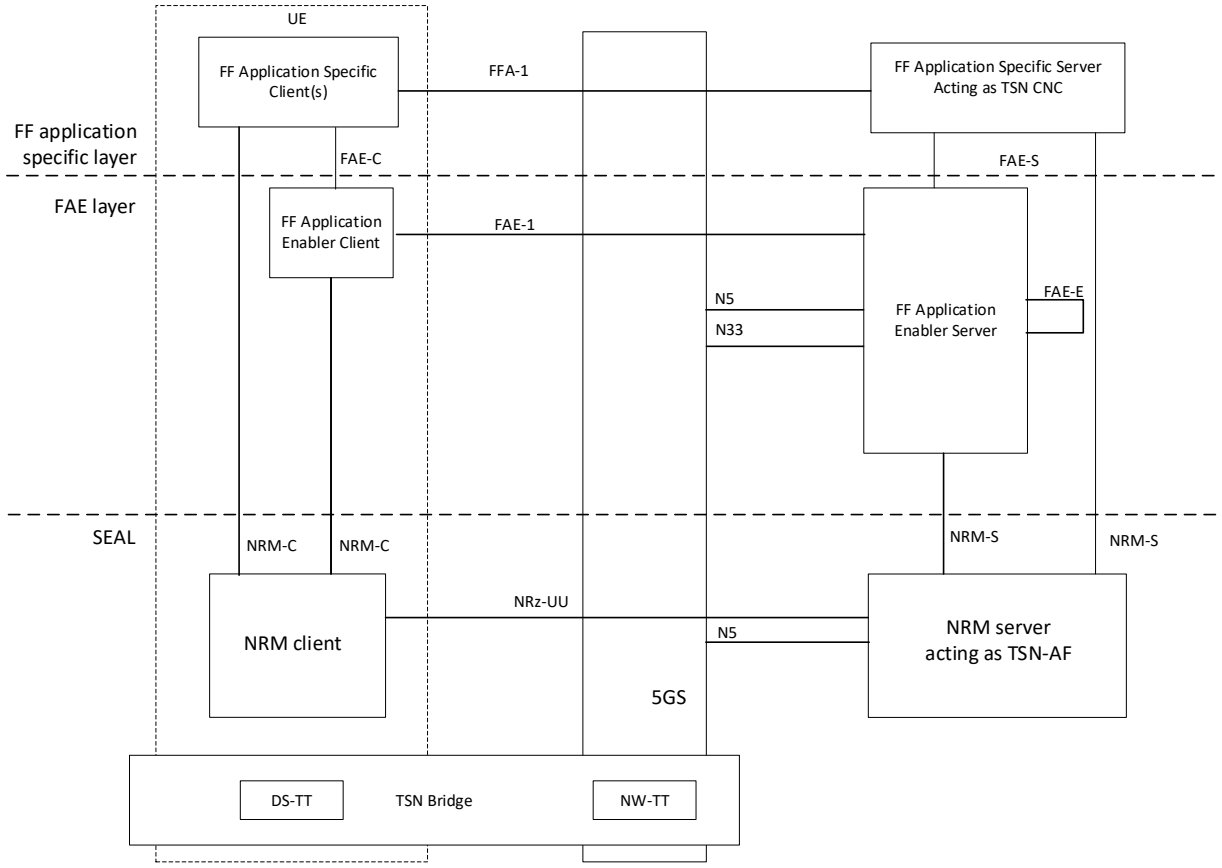

Figure 7.22.2-1: Functional model to support TSN in the SEAL layer

The architecture for the 5G-native TSC is depicted in Figure 7.22.2-2. The SEAL NRM server acts as an AF (referred to as TSC AF) towards the 5G Core Network and performs coordination of QoS flows to fulfill the end-to-end QoS requirements for the UEs involved in the TSC communication. When QoS monitoring is requested, the SEAL NRM server will also perform coordination of the QoS montoring subscriptions and notifications needed for the end-to-end QoS flows using the mechnisms of Solution #10. Upon request from an FF Application layer server via the NRM-S reference point it configures the TSC end-to-end QoS flows in the 5GS. In line with other SEAL service enablers the SEAL NRM server provides a RESTful interface on the NRM-S reference point. As a TSC AF the SEAL NRM server interacts with the 5GS PCF over the N5 reference point to configure the 5G QoS and TSCAI parameters in the 5GS. UE-TSC corresponds to UE-DS-TT in the TSN integration case, which also means that UE-TSC residence time is the same as UE-DS-TT residence time that is used for the end-to-end latency calculation.

NOTE: The NRM server uses procedures of the N5 reference point specified in Rel-16.

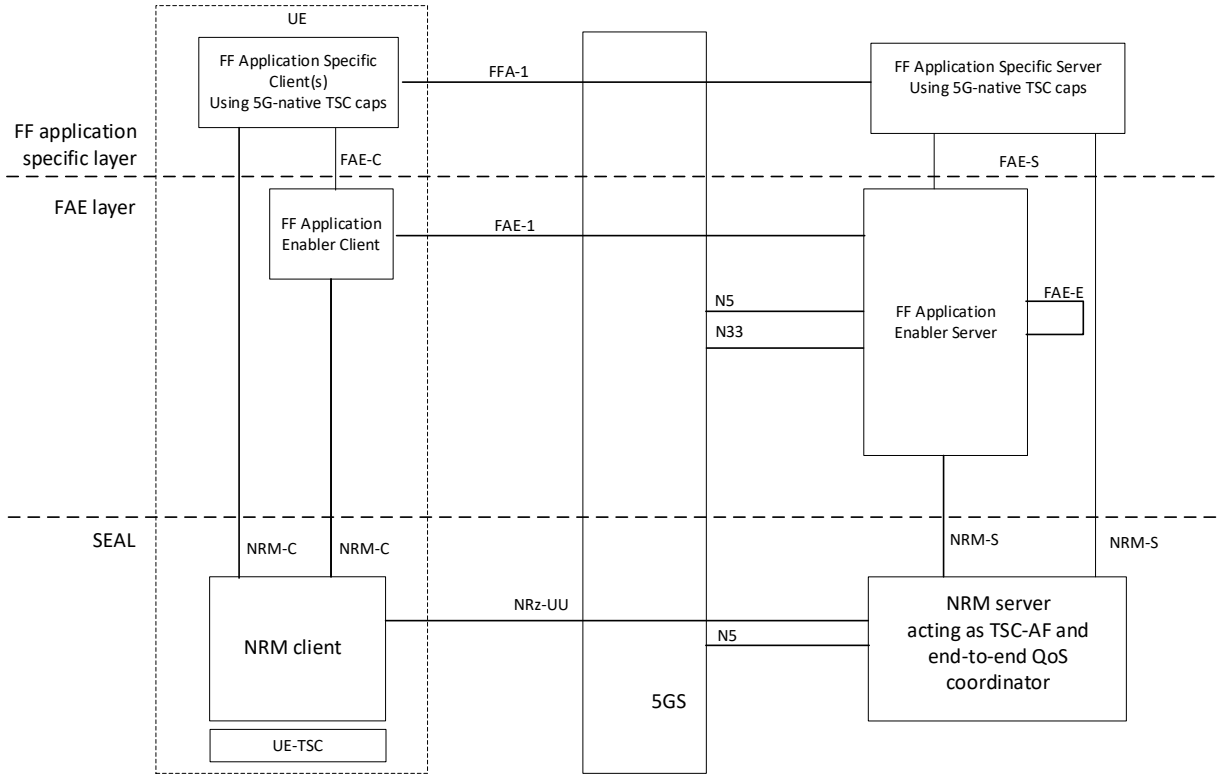

Figure 7.22.2-2: Functional model to support 5G-native TSC in the SEAL layer

7.22.3 5G-native TSC procedures

7.22.3.1 TSC stream discovery procedure

Pre-conditions:

1. UE-TSCs are assigned to a VLAN and each UE has an established Ethernet PDU session.
2. The TSC-AF has populated the NRM server management information base (defined in IEEE 802.1Qcc [25] with the 5G bridge management and port management information. The latter is related to the Ethernet ports located in the UE-TSCs including bridge delay per UE-TSC Ethernet port pair per traffic class.
3. NRM server acting as TSC AF has calculated the bridge delay for each port pair, i.e. composed of (ingress UE-TSC Ethernet port, egress UE-TSC Ethernet port) including the UE-DS-TT residence time, PDB and propagation delay for both UL from sender UE and DL to receiver UE.

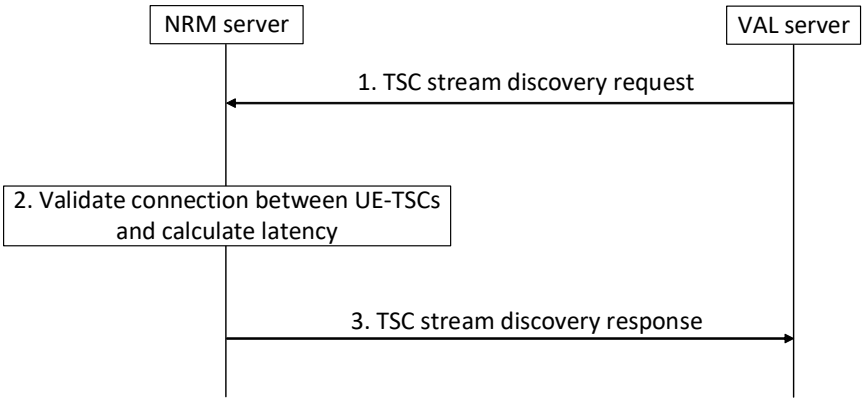

Figure 7.22.3.1-1: TSC stream discovery procedure

1. The NRM server receives a request from a VAL server on NRM-S reference point to discover the connectivity and available QoS characteristics between UE-TSCs identified by their MAC addresses. The request includes Stream ID (as defined in IEEE 802.1CB [37]), source UE-TSC port MAC address and destination UE-TSC port MAC address.

2. The NRM server validates the connectivity between the UE-TSCs connected in the same VLAN based on the stored managed objects info base, identifies the traffic classes supported by the UE-TSCs and calculates the end-to-end latency (including the residence time of the UE-DS-TTs, PDBs, and propagation delay).

3. NRM server responds to the VAL server with the Stream ID and the available end-to-end latency and the traffic classes supported by the UE-TSCs.

7.22.3.2 TSC stream creation procedure

This procedure allows the VAL application to create a TSC stream.

Pre-conditions:

1. Each UE has an established Ethernet PDU session for its UE-TSC port MAC address.

2. Each NRM Client has an established connection with the NRM server.

3. Connectivity between the UE-TSCs has been validated by the TSC stream discovery procedure.

4. NRM server maintains mapping from the traffic class to TSC QoS (including latency).

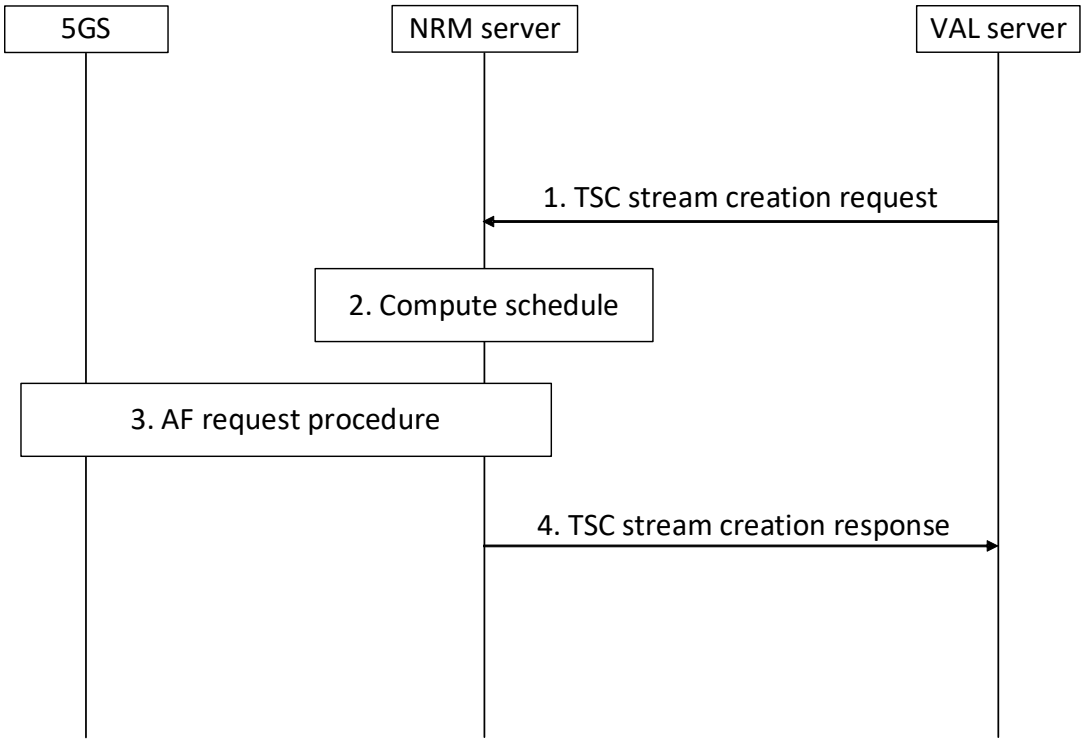

Figure 7.22.3.2-1: TSC stream creation procedure

1. NRM server receives a TSC stream creation request from a VAL server (FAE or FF application specific server) to create a TSC stream identified by a Stream ID, between UE-TSC ports for a traffic class (e.g. scheduled traffic, strict priority) and traffic specification including MaxFrameInterval, MaxFrameSize, MaxIntervalFrames, MaxLatency, etc., as described in IEEE 802.1Qcc [25] in clause 46.2. If QoS monitoring is requested, the SEAL NRM server will also perform coordination of the QoS montoring subscriptions and notifications needed for the end-to-end QoS flows using the mechnisms of Solution #10.

2. NRM server calculates the schedule for the Stream ID. It provides per-stream filtering and policing parameters according to IEEE 802.1Q [6] used to derive the TSC QoS information and related flow information. NRM server also provides the forwarding rule according to IEEE 802.1Q [6] used to identify the UE-TSC MAC

address of the corresponding PDU session. Based on the 5GS bridge delay information it determines the TSC QoS information and TSC Assistance information for the stream.

3. NRM server triggers via N5 the AF request procedure as shown in 3GPP TS 23.502 [12] annex F.2 for the TSC stream for both UL QoS flow (sender UE to UPF/bridge) and DL QoS flow (UPF/bridge to receiver UE). The AF request includes the Stream ID, the UE-TSC port MAC address, TSC QoS information, TSC Assistance Information, flow bit rate, priority, Service Data Flow Filter containing flow description including Ethernet Packet Filters. The QoS flow will be assigned for the PDU session for the source MAC address for the UL direction and for the PDU session for the destination MAC address for the DL direction. The configuration sent over N5 includes also the gate control list (including AdminControlList, AdminBaseTime, AdminCycleTime and Tick Granularity) for the Stream ID. The gate control parameters are for the hold and forward buffering by the UE-TSC for the respective TSC flow. This information is delivered to the UE-TSC by the 5GS.
4. NRM server sends TSC stream creation response to the VAL server with the result of TSC stream creation for the Stream ID.

7.22.3.3 Void

7.22.3.4 Void

7.22.3.5 TSC stream deletion procedure

This procedure allows the VAL application to delete a TSC stream.

Pre-conditions:

1. The TSC stream is configured in the 5GS and the UE-TSCs.

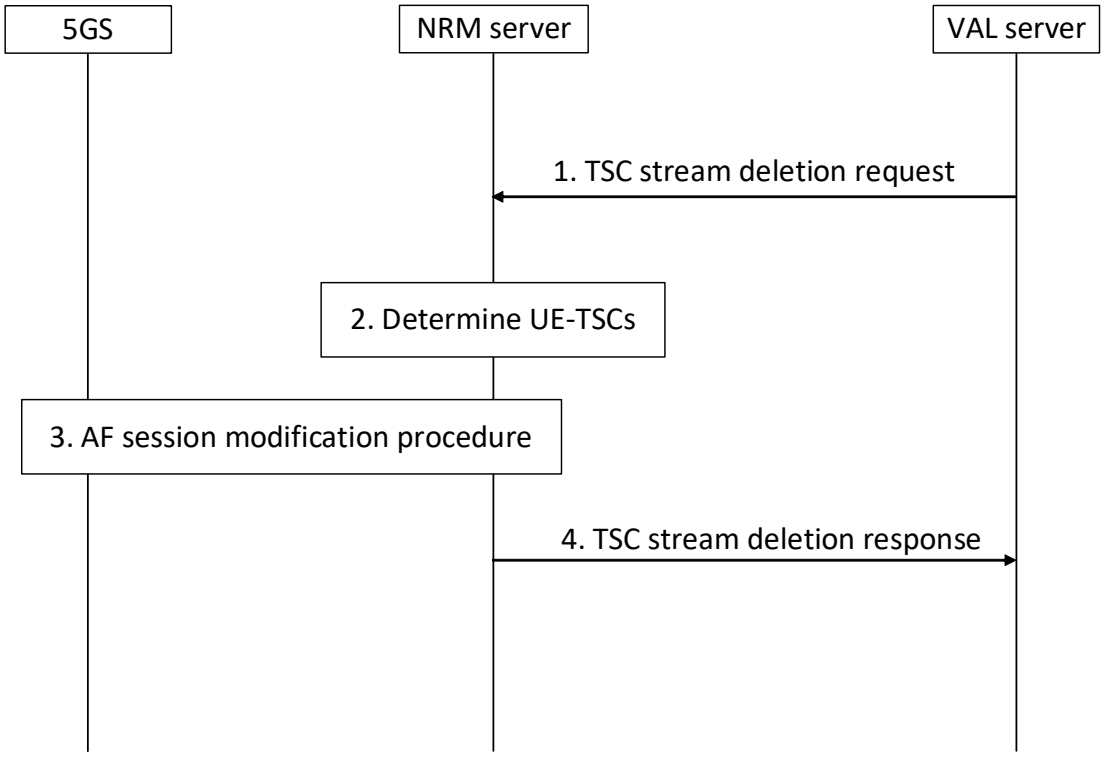

Figure 7.22.3.5-1: TSC stream deletion procedure

1. NRM server receives a request from VAL server to delete a TSC stream for with a Stream ID.
2. NRM server identifies the MAC addresses of the UE-TSCs and the NRM clients involved in the stream based on the stored information for the Stream ID.

3. NRM server triggers via N5 the AF session modification procedure defined in 3GPP TS 23.502 [12] clause 4.15.6.6 for MAC address and Stream ID. NRM server uses the procedure to delete both UL QoS flow (sender UE to UPF/bridge) and DL QoS flows (UPF/bridge to receiver UE) from the PDU sessions of the UEs involved in the stream carrying the TSC stream with the Stream ID.

4. NRM server sends TSC stream deletion response to the VAL server with the result of TSC stream deletion for the Stream ID.

7.22.4 IEEE-TSN TSC procedures

7.22.4.1 5GS TSN Bridge information reporting

Pre-conditions:

1. VAL server (FAE server or FF application specific server) acts as TSN CNC.

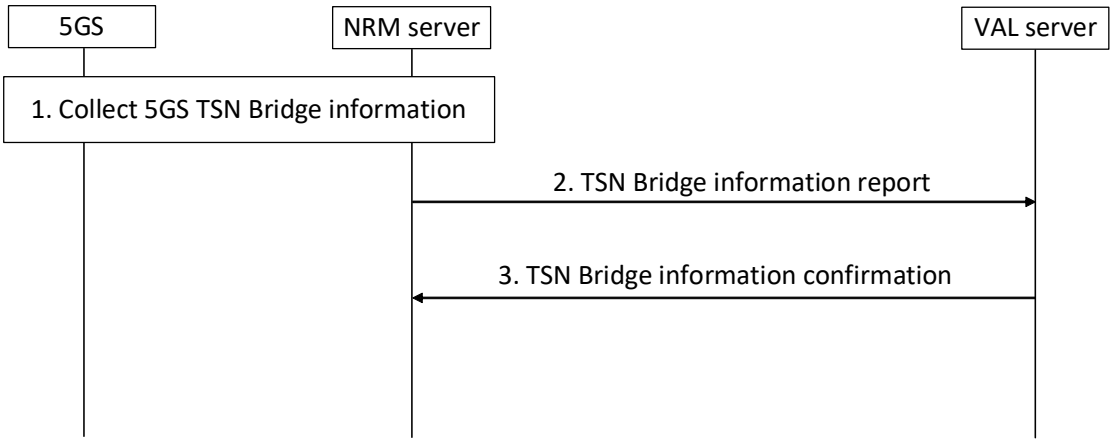

Figure 7.22.4.1-1: TSN Bridge information reporting procedure

1. Acting as the TSN AF the NRM server collects 5GS TSN Bridge information by interaction with the 5GS via the N5 reference point, as described in in TS 23.502 [12] Annex F.1. The NRM server stores the binding relationship between 5GS Bridge ID, MAC address of the DS-TT Ethernet port and also updates 5GS bridge delay as defined in clause 5.27.5 of TS 23.501 [2]. The NRM server retrieves txPropagationDelay and Traffic Class table from DS-TT and it also retrieves txPropagationDelay and Traffic Class table from NW-TT.

2. The NRM server constructs the above received information as 5GS TSN Bridge information and sends them to the VAL server acting as CNC to register a new TSN Bridge or update an existing TSN Bridge.

3. The VAL server stores the TSN Bridge information and returns a confirmation to the NRM server.

7.22.4.2 5GS TSN Bridge configuration procedure

Pre-conditions:

1. VAL server (FAE server or FF application specific server) acts as TSN CNC and it has stored the 5GS TSN Bridge information received from the NRM server acting as TSN AF.

2. The NRM server acting as TSN AF has stored the 5GS TSN Bridge information collected from the 5GS, as described in clause 7.22.4.1.

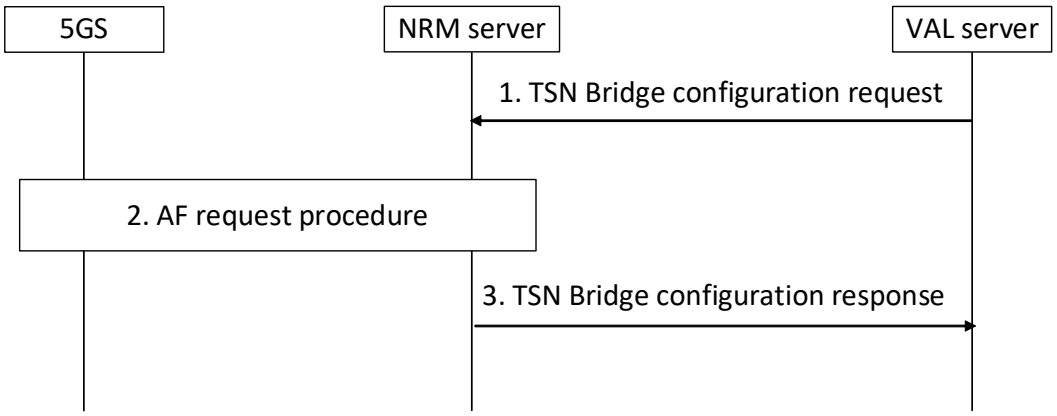

Figure 7.22.4.2-1: TSN Bridge configuration procedure

1. The NRM server receives from the VAL server acting as CNC per-stream filtering, policing parameters and related flow information according to IEEE 802.1Q [6] and it uses them to derive TSN QoS information and related flow information. The TSN AF uses this information to identify the DS-TT MAC address of the corresponding PDU session.
2. NRM server triggers via N5 the AF request procedure as described in 3GPP TS 23.502 [12] Annex F.2. The AF request includes the Stream ID, the UE-DS-TT port MAC address, TSC QoS information, TSC Assistance Information, flow bit rate, priority, Service Data Flow Filter containing flow description including Ethernet Packet Filters.
3. NRM server sends a TSN Bridge configuration response.

7.22.5 Solution evaluation

This is a viable technical solution for aspects related to Key Issue #4 on TSN support, Key Issue #11 on QoS coordination, and Key Issue #8 on communication of FF application requirements, where common support for integration with TSN and for 5G-native (i.e. non-TSN) use cases is provided by enhancing the SEAL NRM enabler service.

For the 5G-native case, the solution builds on top of the capabilities provided by 5G CN in Rel-16 and adds support for end-to-end TSC service between UEs within the 5GS, providing required coordination of the QoS flows, so that these supporting mechanisms can be utilized by VAL servers.

For the TSN integration case, the solution is aligned with the TSN integration solution specified by SA2 in Rel-16. NRM server acts as TSN AF and supporting mechanisms can be utilized by VAL servers. There are no additional IEs necessary for the NRM server acting as a TSN AF.

The NRM server of SEAL takes the role of TSN AF and TSC AF and is part of 5GC as specified in TS 23.501 [7].

7.23 Solution #23 (merging Sol#5, #6): Edge computing for FFAPP

7.23.1 Solution description

This solution corresponds to the key issue #9 - communication service on the Edge deployments and merges sol#5 and sol#6 with a complete analysis.

The EDGEAPP architecture is specified in 3GPP TS 23.558 [10]. The EDGE-5 reference point details are not specified in Rel-17.

Figure 7.23.1-1 illustrates the edge deployment example for the FFAPP. For simplicity, the reference points between enabler server and 5GS are omitted, and the reference points for inter-enabler server communication in the same enabler layer are also omitted. At UE side, FF Application Specific client(s) and FAE client interact with the Edge Enabler Client (EEC) via EDGE-5 reference point. In an Edge Data Network (EDN), the Edge Application Server (EAS), e.g.

FF Application Specific Server and FF Application Enabler server, interacts with the Edge Enabler Server (EES) via EDGE-3 reference point, for instance, to register its profile into the EES. The EEC interacts with the Edge Configuration Server (ECS) via EDGE-4 reference point, for instance, to discover candidate EES(s). The EEC interacts with the EES via EDGE-1 reference point, for instance, to discover candidate EAS(s) (e.g. FF Application Specific Server and FF Application Enabler Server) and provide the discovered EAS(s) to the Application Client (e.g. FF Application Specific client and FF Application Enabler client).

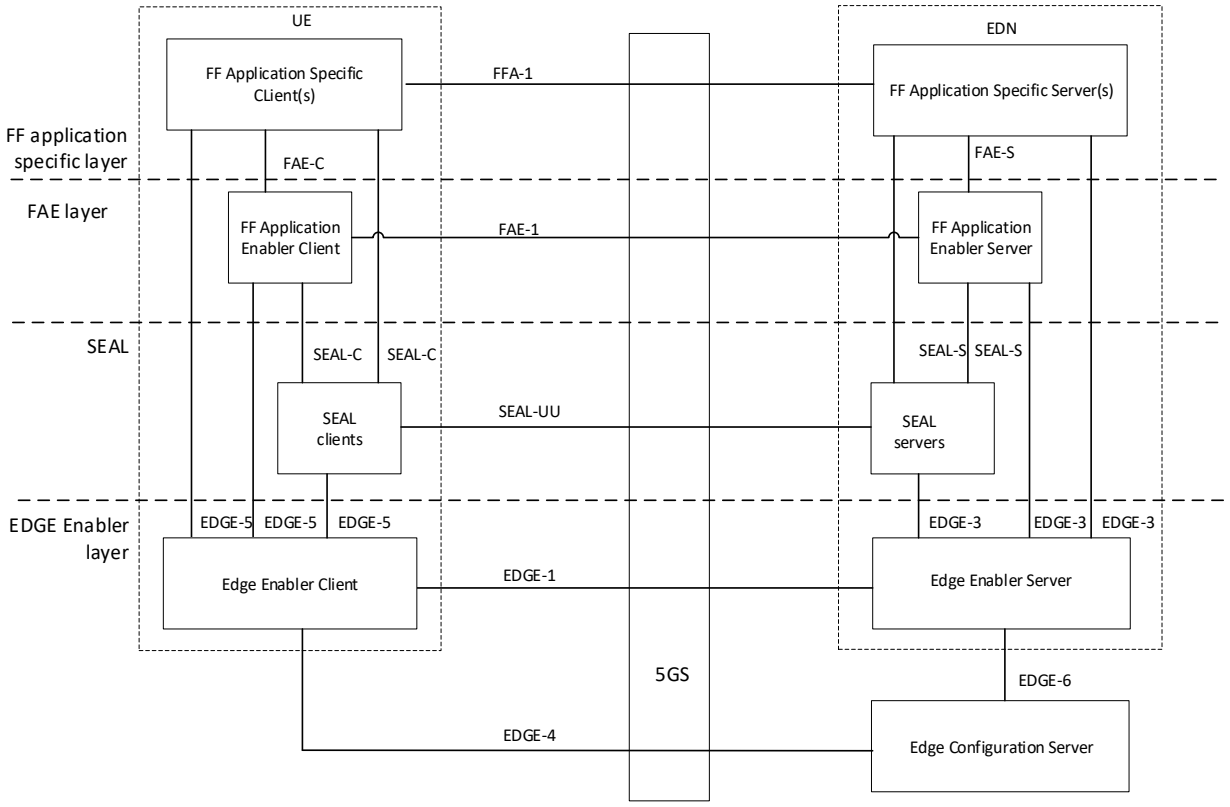

Figure 7.x.1-1: FFAPP in EDGE deployment

In an EDN, there could be several EES(s) provided by the same or different ECSP. The FF application specific server(s) and FAE server shall be able to discover and register into an appropriate EES. If CAPIF is used, this can be done by utilizing the AEF serving area and/or the AEF location as described in 3GPP TS 23.222 [16]; otherwise, local configuration of the EES endpoint may be used.

Note that the other EDGE-3 exposure services are not re-exposed by the FAE server or SEAL servers to the FF application specific server, for instance, the FF application specific server directly consumes location or QoS API provided by the EES.

Editor's note: Within an edge deployment, if the application enabler client in the UE and application specific server need to communicate with the same application enabler server, whether and how the edge enabler layer is impacted is FFS.

7.23.2 Solution evaluation

This solution addresses KI#9 for "How to support FFAPP communications over Edge deployments" and provides a deployment option for the FF application in the EDGE application architecture.

7.24 Solution #24: Message communication using MSGin5G service

7.24.1 Introduction

This solution addresses Key Issue #18 on Support for Message communication.

The MSGin5G Service has been studied in 3GPP TS 23.700-24 [39]. The MSGin5G architecture has been defined to support following capabilities requirements as specified in clause 7.1.2 of TS 23.700-24 [39].

- [AR-7.1.2-a] The application architecture shall enable deployment of MSGin5G UE which are of heterogeneous nature including light weight constrained devices (e.g. sensors, actuators) and unconstrained devices with advanced capabilities (e.g. washing machine, micro-ovens).

- [AR-7.1.2-c] The application architecture shall enable the communication payload size varying from small data message to large data message.

Further, the solutions has been studied and concluded to support MSGin5G service requirements related to one to one, group and broadcast message services for thing-to-thing and person-to-thing communication with low end-to-end latency and high reliability of message delivery, in a resource efficient manner.

The sensors and actuators are also used in factory automation and as mentioned in KI#18 – similar message communication requirements are applicable for FFAPP also.

7.24.2 Solution description

The architecture for MSGin5G service has been specified in clause 8.2 of 3GPP TR 23.700-24 [39]. For non-TSN communications,

- the UE in FFAPP architecture acts as MSGin5G UE-1 in MSGin5G architecture; however, the UE in FFAPP architecture do not act as message gateway which is defined for MSGin5G UE-1 in MSGin5G architecture;

- the FAE client in FFAPP architecture acts as MSGin5G client in MSGin5G architecture;

- the FAE server may implement MSGin5G server functionalities as specified in MSGin5G architecture; and

- the solutions studied and concluded in 3GPP TR 23.700-24 [39] for one-to-one, group and broadcast messages are applicable for FFAPP also, except solution# 28 which involves message gateway functionalities of the MSGin5G UE-1.

7.24.3 Solution evaluation

This solution provides details on reusing MSGin5G architecture and solutions for FFAPP for non-TSN messaging communications.

8 Overall evaluation

8.1 General

The following subclauses contain an overall evaluation of the solutions presented in this technical report, and their applicability to the identified key issues.

- Clause 8.2 provides an evaluation of the high level architecture specified in clause 7.1 & 7.3; and

- Clause 8.3 lists the solutions for the key issues including impact on other working groups that will need consideration.

8.2 Architecture evaluation

The architecture solution in clause 7.1 describes the functional model for FF application layer. The solution in clause 7.3 describes supporting UE to UE direct communication in FF application layer. The solutions in clause 7.16 and clause 7.22 describes functional models for supporting TSN communications. A summary of the architecture and key issues specified in this technical report are listed in table 8.2-1.

Table 8.2-1: Architecture evaluation

Architecture solution	Applicable key issues (subclause reference)	Evaluation (subclause reference)	Dependency on other working groups
Solution #1: FF application layer functional model	Supports key issues 1~12 & 13~15 specified in clause 5		SA2
Solution #3: Support UE to UE direct communication in FF application layer	Supports key issues 8~10 & 15 specified in clause 5		SA2
Solution#16: TSN policy negotiation via FAE layer	Supports key issue 4 specified in clause 5		SA2
Solution#22: SEAL support for TSC services	Supports key issues 4, 8 and 11 specified in clause 5.		

For supporting non-TSN communications, solution#1 provides a viable functional model, where FAE server provides application support functions.

For supporting direct UE-to-UE communications, solution#3 provides a viable functional model, where FAE clients support such interactions.

For supporting TSN communications, solution#16 provides a viable functional model where the role of TSN AF is assigned to the FAE server.

Solution#22 provides a viable functional model for both the TSN and TSC (non-TSN) cases, where the role of TSN AF and TSC AF is assigned to SEAL's NRM server.

As per 3GPP TS 23.501 [7], TSN AF is part of 5GC. Any functional entity defined in the functional model for FFAPP and assumes the role of TSN AF shall be compliant with the related architecture constraints specified in 3GPP TS 23.501 [7].

It is recommended that the architecture solutions for supporting TSN communications and TSC caters to multiple vertical applications and hence a solution in SEAL is favorable.

8.3 Key issue and solution evaluation

8.3.1 General

All the key issues and solutions specified in this technical report are listed in table 8.3-1. It includes the mapping of the key issues (clause 5) to the solutions and corresponding solution evaluations. Also it lists the dependency on the ongoing work in the other working groups that will need consideration during the normative phase.

Table 8.3-1: Key issue and solution evaluation

Key issue	Solution	Impact on FAE layer	Impact on SEAL layer	Evaluation (subclause reference)	Dependency on other working groups
Key issue 1 - Use of network slicing for FFAPP	Solution #12: Private Slice		Yes NRM or new	7.12.2	SA2, SA5
	Solution #13: Application-triggered slice re-mapping for FF applications	Yes	Yes NRx	7.13.2	SA2, SA5
Key issue 2 - Geographic location and positioning information support	Solution #7 Geographic location and positioning information support		Yes LM	7.7.5	
Key issue 3 - Clock synchronization	Solution #14 clock synchronization			7.14.3	SA2
	Solution 15: Time Synchronization Management		Yes NRM	7.15.3	SA2
Key issue 4 - TSN supporting	Solution #16: TSN policy negotiation via FAE layer	Yes	Yes NRx(Solution #10)	7.16.2	SA2
	Solution #17: Support TSN in FF Application Enabler layer	Yes		7.17.2	SA2
	Solution #22: SEAL support for TSC services		Yes NRM	7.22.5	
Key issue 5 - QoS monitoring	Solution #8: QoS monitoring	Yes		7.8.2	SA2
	Solution #10: QoS monitoring for TSC services		Yes NRM	7.10.3	SA2
Key issue 6 - 5GLAN group management	Solution #9: 5GLAN group management		Yes GM	7.9.2	
Key Issue 7 - Device Onboarding				-	SA2
Key issue 8 - Communication of FF application requirements with 5GS	Solution #2: Establishing communication with FF application service requirements	Yes		7.2.2	
	Solution #11: Establishing communication connectivity between FF Enabler Clients with FF application service requirements	Yes		7.11.2	
	Solution #19: Communicating FF application service requirements with 3GPP system		Yes NRM	7.19.2	
	Solution #22: SEAL support for TSC services		Yes NRM	7.22.5	
Key issue 9 - Communication service on the Edge deployments	Solution #5: Edge deployment within FFAPP	Yes		7.5.2	
	Solution #6: Provisioning of FFAPP within Edge Data Network configuration	Yes		7.6.2	
	Solution #23 (merging Sol#5, #6): Edge computing for FFAPP	Yes	Yes	7.23.2	
Key issue 10 - Integration with Existing Operation Technologies	Annex B: Integration with Operation Technologies				
Key issue 11 - QoS coordination	Solution #2: Establishing communication with FF application service requirements	Yes		7.2.2	
	Solution #11: Establishing communication connectivity between FF Enabler Clients with FF application service requirements	Yes		7.11.2	
	Solution #19: Communicating FF application service requirements with 3GPP system		Yes NRM	7.19.2	

Key issue	Solution	Impact on FAE layer	Impact on SEAL layer	Evaluation (subclause reference)	Dependency on other working groups
	Solution #22: SEAL support for TSC services		Yes NRM	7.22.5	
Key Issue 12 - User authorization	SA3 scope				SA3
Key Issue 13: Capability Exposure related to Private Slice Network Status	Solution #12: Private Slice		Yes NRM or new	7.12.2	SA2, SA5
	Solution #1: FF application layer functional model			7.1.2	
Key Issue 14 – Device monitoring	Solution #18: Device monitoring	Yes	Yes NRM	7.18.2	
Key Issue 15 – Support for group communication	Solution #9: 5GLAN group management		Yes GM	7.9.2	
Key Issue 16 – Constrained devices	Solution #20: SEAL support for CoAP to address constrained devices		Yes	7.20.6	
Key Issue 17 – Using 5G CN capabilities for SEAL Groups	Solution #21: Enabling 5G CN capabilities for SEAL Groups		Yes GM	7.21.3	
Key Issue 18 – Support for Message communication	Solution #24: Message communication using MSGin5G service	Yes		7.24.3	

8.3.2 Overall evaluation of solutions for key issue#1

Key issue#1 corresponds to use of network slicing for FFAPP. Two solutions are proposed in this document.

Solution #12 proposes to enhance SEAL to support NEF or EGMF for acquiring private slice network status information. Solution#12 is about using existing slicing functionalities via SEAL or FAE server. No additional requirements are expected from SA2 or SA5.

Solution #13 proposes to enable the FAE server to translate the adaptation of the service requirements / profile, as triggered by the FF application specific server or client, to a network slice re-mapping. Solution#13 is also based on existing services from 5GC.

For the open issue on whether the slicing support functions specified by SA5 and SA2 are sufficient for FFAPP requirements, no additional functions are foreseen by SA5 and SA2 in this Release for supporting FFAPP requirements.

Solution#12 will be considered for normative work to be part of SEAL as the proposed solution addresses the generic service requirements common across different verticals. Solution#13 is a candidate SEAL solution, but it is not technically feasible due to unresolved dependencies on SA2-defined capabilities and cannot be considered for normative work until those dependencies and/or potential overlaps are resolved.

8.3.3 Overall evaluation of solutions for key issue#2

Key issue#2 corresponds to geographic location and positioning information support for FFAPP. One solution is proposed in this document.

Solution #7 proposes to enhance SEAL location management to support FFAPP geographic location and high accuracy positioning requirements.

For issue 1, the following positioning non-3GPP positioning technologies are available: GNSS (e.g. Beidou, Galileo, GPS, Glonass), Network-based Assisted GNSS and High-Accuracy GNSS, Terrestrial Beacon Systems, dead-reckoning sensors (e.g. IMU, barometer), WLAN/Bluetooth-based positioning. The selection of which positioning technology to use for each FFAPP scenario is up to implementation. A possible use of these are captured in solution#7.

For issue 2, there is no solution for positioning method with ms-level latency in this study.

For issue 3, there is no solution for absolute and relative positioning in this study.

For issue 4, solution#7 proposes to enhance SEAL LMS to support FFAPP location acquisition and location reporting scenarios.

Solution#7 can be considered for normative work as the proposed solution addressing the service requirements for different verticals. Positioning methods for ms-level latency and absolute and relative positioning are not yet supported in Solutuon #7 and will not be included in normative work.

8.3.4 Overall evaluation of solutions for key issue#3

Key issue#3 corresponds to manage and utilize 5G clock synchronization mechanism for FFAPP. Two solutions are proposed in this document.

For issue a, no additional mechanism is required for managing and utilizing 5G clock as specified in 3GPP TS 23.501 [7].

For issue b, the APIs are provided by NEF. There are no additional enhancement to SEAL to support these APIs. The impact on SEAL for using these APIs require further study can be assessed during normative work.

Solution #14 proposes to use TSN time synchronization mechanisms specified by SA2 and no need normative work.

Solution #15 proposes to enhance SEAL to expose the Time synchronization capabilities obtained from NEF via N33 to Application Specific Servers that need to use the Time Synchronization Service.

Solution #15 will be considered for normative work if the proposed solution addresses the generic service requirements common across different verticals considering the functionalities provided by NEF.

8.3.5 Overall evaluation of solutions for key issue#4

Key issue#4 corresponds to TSN support of and translation of TSN application QoS requirements to network QoS parameters of FF applications within the 5G network. Three solutions are proposed in this document.

Solution#16 proposes that a trigger event - based on the monitored QoS parameters (by SEAL / NRx or by the network) - which can be a policy related to the 1) adaptation of application requirements (e.g. survival time, TSC service area, mobility change) or 2) adaptation of port management policies (DS-TT, NW-TT policies) makes the TSN system to provide a request for adaptation of the configuration based on these requirements, and FAE server will send these policies to the corresponding Devices (FAE clients). There is no valid use case identified for this solution.

Solution#17 proposes to support FAE server acting as TSN AF without SEAL, which depends TSC capabilities specified on Rel-16 3GPP TS 23.501 [7] and solutions currently studied in 3GPP TR 23.700-20 [13].

Solution#22 proposes an architecture to expose Time Sensitive Communication (TSC) capabilities of the 5G system which supports integration with an IEEE TSN system as well as 5G-native (i.e. non-TSN) TSC services. Due to the common nature of these TSC capabilities (which can be used by various verticals), it is proposed to enhance the SEAL.

Solution#22 will be considered for normative work as the proposed solution addresses the generic service requirements common across different verticals. It provides a solution at the SEAL enabling layer compared to Solutions #16 and #17 which are only applicable for FF applications.

8.3.6 Overall evaluation of solutions for key issue#5

Key issue#5 corresponds to the QoS monitoring capabilities of the 5G network. 2 solutions are proposed in this document.

Solution#8 proposes to address the issue via the NEF, according to the procedures defined in 3GPP TS 23.502 [12] clause 4.15. NEF supports APIs of exposure of network events, analytics for QoS monitoring.

Solution#10 proposes a solution where the SEAL NRM service enabler is enhanced with QoS monitoring. The NRM service will make use of the NEF QoS monitoring capabilities.

As the QoS monitoring requirements are not specific to FFAPP, it is therefore better supported in the common SEAL layer to also address other verticals, as also recommended in the evaluation of Solution #8 in clause 7.8.2.

8.3.7 Overall evaluation of solutions for key issue#6

Key issue#6 corresponds to 5GLAN group management for FFAPP. One solution is proposed in this document.

For issue a & issue b, solution#9 addresses these issues.Solution #9 proposes to enhance SEAL group management service to handle 5GLAN groups based on 5G core network capabilities.

Solution #9 will be considered for normative work as the proposed solution addresses the generic service requirements common across different verticals.

8.3.8 Overall evaluation of solutions for key issue#7

Key issue#7 corresponds to Device onboarding for FFAPP. There is no solution proposed in this document.

For issue a, no solution was proposed for this open issue.

For issue b, annex A captures analysis of oneM2M and possible relationship with FFAPP.

For issue c, no solution was proposed for this open issue.

Device onboarding is important aspect, which found solutions in SA2 TS 23.501 [7] and SA3 TS 33.501 [40] Rel17 work. If any enhancements are identified for SEAL or FAE server over the existing 5GC capabilities will be considered during normative work.

8.3.9 Overall evaluation of solutions for key issue#8

Key issue#8 corresponds to the communication of FF application requirements with the 5G network. 4 solutions are proposed in this document.

Solution#2 proposes that the application requirements are collected by the FAE server and further the related connectivity is established by translating the application requirements to 3GPP transport requirements and interacting with the underlying 3GPP system.

Solution#11 proposes that application requirements are collected or fetched by the FAE server and further the related connectivity is established by translating the application requirements to 3GPP transport requirements and interacting with the underlying 3GPP system.

Solution#19 proposes to re-use SEAL's NRM server functionality specified in clause 14.3.4 of 3GPP TS 23.434 [8] and enhance it to consider translation of all vertical application requirements to 3GPP system's transport layer requirements.

Solution#22 proposes that application requirements are collected by the SEAL NRM server which exposes Time Sensitive Communication (TSC) capabilities of the 5G system. While the solution supports the non-TSN case (5G-native) which is the subject of KI#8, it also supports the integration with an IEEE TSN system. Due to the common nature of these TSC capabilities (which can be used by various verticals), it is proposed to expose it by the SEAL layer.

The solutions propose the following for the expression of service requirements:

- Solution#2 proposes that the service requirement from the source includes packet size, packet transmission interval, packet processing latency, allowed packet loss rate/packet loss amount/packet error rate, etc.
- Solution#11 and solution#19 do not provide the details of the service requirements.
- Solution#22 proposes to express the service requirements as described in IEEE 802.1Qcc [25], such as traffic class, traffic specification including MaxFrameInterval, MaxFrameSize, MaxIntervalFrames, MaxLatency.

The solutions propose the following for translating the service requirements to transport QoS requirement for communication with the 3GPP core network:

- Solution#2 and Solution#11 specify that FAE server determines the transport QoS requirements given the service requirements as input. Such mechanism is assumed to be as per implementation usually considering the mapping of the service requirements to 3GPP transport QoS requirements specified by SA1.
- Solution#19 specifies that NRM server should be responsible for such translation between service requirements and transport QoS requirement to communication with 3GPP core network.

- Solution#22 specifies that the NRM server determines the transport QoS requirements based on the service requirements in line with IEEE 802.1Qcc [25].

Solution#22 can be considered for normative work as the proposed solution addresses the generic service requirements common across different verticals. It provides a solution at the SEAL enabling layer compared to Solutions #2 and #11 which are only applicable for FF applications.

Further work during normative phase can consider whether and how the mechanisms proposed by solution#2 and solution#11 can be introduced in SEAL by possibly generalizing the application/service requirements across the verticals.

8.3.10 Overall evaluation of solutions for key issue#9

Key issue#9 corresponds to FFAPP communication service on the Edge deployments. Three solutions are proposed in this document.

For first issue, solutions 5, 6 and 23 provide solutions for this issue.

For second issue, no solutions are proposed for this issue.

Solution #5 proposes to provide a deployment option for FAE client and FAE server considering edge enabler layer.

Solution #6 proposes to provision with Edge Data Network deployment for FFAPP.

Solution #23 merges solution#5 and solution #6, proposes to provide deployment for the FF application in the EDGE application architecture.

Solution #23 will be considered for normative work as the proposed solution completely addresses the edge deployment requirements of key issue#9.

8.3.11 Overall evaluation of solutions for key issue#10

Key issue#10 corresponds to integrate with existing operation technologies for FFAPP.

For first issue, the OTs are identified in Annex B and C.

For second and third issues, the integration and specification of OT with FFAPP will be considered in normative phase.

There is no solution proposed in this document, but an analysis is performed in Annex B. Further work during normative phase can consider this analysis for integration with existing operation technologies.

8.3.12 Overall evaluation of solutions for key issue#11

Key issue#11 corresponds to the QoS coordination method to support QoS based communications for one or more FFAPP applications between the devices when not using TSN. Four solutions are proposed in this document.

Solution#2 proposes that the application requirements are collected by the FAE server and the related connectivity is further established by translating the application requirements to 3GPP transport requirements and interacting with the underlying 3GPP system.

Solution#11 proposes that application requirements are collected or fetched by the FAE server and further the related connectivity is established by translating the application requirements to 3GPP transport requirements and interacting with the underlying 3GPP system.

Solution#19 proposes to re-use SEAL's NRM server functionality specified in clause 14.3.4 of 3GPP TS 23.434 [8] and enhance it to consider translation of all vertical application requirements to 3GPP system's transport layer requirements.

Solution#22 proposes that the SEAL NRM server supports management of the end-to-end QoS flows in the 5GS. This will enable an FF application to request configuration of TSC QoS flows between UEs within the 5GS via the NRM-S reference point. The SEAL NRM server will perform QoS coordination for the set of UEs and their respective QoS flows. In this case the NRM-S reference point will specify a 3GPP protocol for this interaction. The NRM server will interact with the 5GC via N5 reference point as specified in 3GPP TS 23.501 [7].

Solution#22 will be considered for normative work as the proposed solution addresses the generic service requirements common across different verticals. The mechanisms provided by Solutions #2 and #11 for communication of non-TSN QoS requirements can be considered for normative work.

8.3.13 Overall evaluation of solutions for key issue#12

Key issue#12 corresponds to user consent for FFAPP. The solution for key issue#12 is out of scope of SA6 and there is no solution proposed in this document.

8.3.14 Overall evaluation of solutions for key issue#13

Key issue#13 corresponds to capability exposure related to private slice network status and CAPIF usage for service APIs. Two solutions are proposed in this document.

For first issue, no additional service APIs were identified. Solution#12 proposes to use existing 5GC APIs.

For second issue, Solution#1 provides architectural view of integrating FFAPP with CAPIF. No enhancements to CAPIF or SEAL were identified.

Solution #12 proposes to enhance SEAL to support NEF or EGMF for acquiring private slice network status information.

Solution #1 proposes to provide the architecture and functional model required for addressing the application layer support aspects, the CAPIF function is supported in FFAPP functional model.

Solution#12 will be considered for normative work if the proposed solution addresses the generic service requirements common across different verticals by utilizing information from 5GC and 5G management system.

Solution#1 will be considered for normative work as the proposed solution addresses a viable functional model for FF application architecture.

8.3.15 Overall evaluation of solutions for key issue#14

Key issue#14 corresponds to device monitoring for FFAPP. One solution is proposed in this document.Solution #18 proposes to enhance SEAL network resource management service to support device monitoring. For open issue, solution#18 uses existing 5GC APIs. No additional events are proposed. The impact on SEAL or FFAPP will be determined during normative work.

Solution#18 will be considered for normative work if the proposed solution addresses the generic service requirements common across different verticals considering the enhancement of SEAL to support the monitoring events.

8.3.16 Overall evaluation of solutions for key issue#15

Key issue#15 corresponds to support group communication for FFAPP. One solutions is proposed in this document.

For first issue, no solutions were proposed. Any impact on NRM will be determined during normative phase.

For second issue, solution#9 addresses this issue.

Solution #9 proposes to enhance SEAL to support FF application broadcast/multicast group communication operations and group management capabilities.

Solution #9 will be considered for normative work as the proposed solution addresses the generic service requirements common across different verticals.

8.3.17 Overall evaluation of solutions for key issue#16

Key issue#16 corresponds to support for the use of constrained devices for FFAPP. One solution is proposed in this document.Solution #20 proposes to enhance SEAL functional model for the signalling control plane by adding support of CoAP to address constrained devices.

For first issue, solution #20 addresses this aspect for introducing CoAP support for FFAPP.

For second issue, solution #20 proposes signalling layer enhancement of SEAL to support CoAP.

Solution #20 will be considered for normative work with enhancement required for considering architecture support for light weight protocols like CoAP.

8.3.18 Overall evaluation of solutions for key issue#17

Key issue#17 corresponds to use 5G CN capabilities for SEAL groups. One solution is proposed in this document.

Solution #21 proposes to enhance SEAL GMS supporting the external group identifier (identifying a group of UEs by the 3GPP CN) in SEAL Group Management procedures.

For first issue, solution #21 addresses this KI.

For second issue, no additional mechanisms were identified to be provided by 3GPP CN.

Solution #21 will be considered for normative work as the proposed solution addresses requirements common to various vertical applications.

8.3.19 Overall evaluation of solutions for key issue#18

Key issue#18 corresponds to support message communication for FFAPP. One solution is proposed in this document.

Solution #24 proposes to reuse MSGin5G architecture and solutions for FFAPP for non-TSN messaging communications. Though there is a relationship between FFAPP and MSGin5G as per solution #24, whether and how to integrate MSGin5G with FFAPP architecture will be determined during normative phase. It may not be necessary to integrate MSGin5G for FFAPP as specified in solution #24.

Solution #24 will be considered for normative work with suitable enhancements by utilizing MSGin5G capabilities to address requirements for non-TSN messaging communications.

9 Conclusions

Editor's Note: This clause is intended to list conclusions that have been agreed during the course of the study item activities.

The following solutions address corresponding key issues described in clause 5. Therefore, these solutions can be considered for follow-up normative work, respectively.

1) The solution for 5GLAN group management described in clause 7.9 can be considered as a candidate solution on SEAL layer with necessary enhancements as appropriate, according to the overall evaluation (clause 8);

2) The solution for constrained devices described in clause 7.20 can be considered as a candidate solution on SEAL layer with necessary enhancements as appropriate, according to the overall evaluation (clause 8);

3) The solution for enabling the 5G CN capabilities for SEAL Groups in clause 7.21 can be considered as a candidate solution on SEAL layer with necessary enhancements as appropriate, according to the overall evaluation (clause 8);

4) The solution for FF application layer functional model described in clause 7.1 can be considered as the baseline functional model with necessary enhancements as appropriate;

5) The solution for geographic location and positioning information support described in clause 7.7 can be considered as a candidate solution on SEAL layer with necessary enhancements as appropriate, according to the overall evaluation (clause 8);

6) The solution for private slice described in clause 7.12 can be considered as a candidate solution on SEAL layer with necessary enhancements as appropriate, according to the overall evaluation (clause 8);

7) The solution for time synchronization management described in clause 7.15 can be considered as a candidate solution on SEAL layer with necessary enhancements as appropriate, according to the overall evaluation (clause 8);

8) The solution for edge computing described in clause 7.23 can be considered as a candidate solution on FAE layer and SEAL layer with necessary enhancements as appropriate, according to the overall evaluation (clause 8);

9) The solution for Message communication support for non-TSN messaging communications described in clause 7.24 can be considered as a candidate solution on FAE layer with necessary enhancements as appropriate, according to the overall evaluation (clause 8);

10) The solution for QoS monitoring capabilities of the 5G network described in clause 7.10 can be considered as a candidate solution on SEAL layer with necessary enhancements as appropriate, according to the overall evaluation (clause 8);

11) The solution described in clause 7.22 can be considered as a candidate solution on SEAL layer with necessary enhancements as appropriate, according to the overall evaluation (clause 8), for the following requirements:

    1) TSN support and translation of TSN application QoS requirements to network QoS parameters of FF applications within the 5G network;

    2) Communication of FF application requirements with the 5G network;

12) The solution for device monitoring described in clause 7.18 can be considered as a candidate solution on SEAL layer with necessary enhancements as appropriate, according to the overall evaluation (clause 8);

13) The solutions for establishing communication with FF application service requirements described in clause 7.2 and clause 7.11 can be considered as candidate solutions with necessary enhancements (e.g. as SEAL solutions) as appropriate, according to the overall evaluation (clause 8);

Annex A: Analysis of relationship between oneM2M and FF architecture

Annex A.1 Overview

In oneM2M TS-0001[9], the oneM2M functional architecture comprises the following functions: Application Entity (AE), Common Services Entity (CSE), Underlying Network Services Entity (NSE).

oneM2M CSE provides services to applications (AE) which are referred to as Common Services Functions (CSFs). The CSFs contained inside the CSE includes such as: Application and Service Layer Management, Communication Management and Delivery Handling, Data Management and Repository, Device Management, Security, Subscription and Notification etc. Those CSFs can support Device onboarding requirement in Factory.

There are 3 different field node (UE) types defined in oneM2M: Application Service Node (ASN), Middle Node (MN) and Application Dedicated Node (ADN). The ASN UE and MN UE consists of both AE (ASN/MN-AE) and CSE (ASN/MN-CSE) function entity. But ADN UE only consists of AE (ADN-AE) function entity.

There are 1 infrastructure node (Server) type defined in oneM2M - Infrastructure Node (IN). The IN server consists AE (IN-AE) and CSE (IN-CSE) function entity.

The relationship between oneM2M architecture function model and FFAPP function model is described in clause Annex A.2.

Annex A.2 Relationship between oneM2M and FFAPP

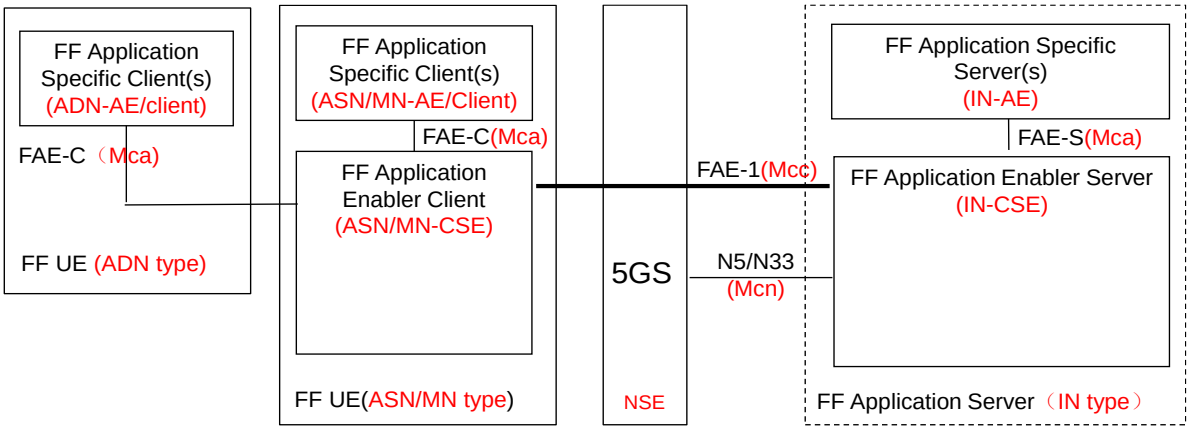

Figure Annex A.2-1: Relationship between oneM2M and FF

Figure Annex A.2-1 shows the corresponding relationship between oneM2M and FFAPP, as follows:

- The oneM2M ASN/MN-CSE (e.g. a Motion Controller or factory automation gateway) function and the FAE client.
- The oneM2M ASN/MN-AE (e.g. a Motion Controller application or factory gateway application) and the FF application specific client.
- The oneM2M ADN-AE (e.g. an Actuator/Sensor in machine) and the FF application specific client.
- oneM2M IN-CSE (e.g. a middleware server) function and the FAE server
- oneM2M IN-AE (e.g. a Motion Control application server) function and the FF application specific server.
- oneM2M NSE function and the 5GS.

- The oneM2M Mca reference point (which defined in oneM2M TS-0001[x]) between AE and CSE in ADN/ASN/MN node and the FAE-C reference point (between FF application specific client and FAE client) in FF UE side.
- The oneM2M Mca reference point (which defined in oneM2M TS-0001[x]) between AE and CSE in IN node and the FAE-S reference point (between FF application specific server and FAE server) in FF application server.
- The oneM2M Mcc reference point between (which defined in oneM2M TS-0001 [x]) ASN/MN-CSE(s) and IN-CSE and the FAE-1 reference point between FAE client and FAE server.
- The oneM2M Mcn reference point (which defined in oneM2M TS-0001[9]) between NSE and IN-CSE and the N5/N33 interface between FAE server and 5G system.

Annex B: Integration with Operation Technologies

B.1 Overview

This analysis corresponds to the key issue #10 on Integration with Existing Operation Technologies.

3GPP TS 22.104 [3] Figure C.5-1 shows a simplified version of the communication stack. The PHY layer, the MAC layer and some parts of the IP layer are part of the 3GPP network. The layers that are part of the 3GPP network are referred to as lower communication layers (LCL). The OSI layers (the transport layer, the session layer, the presentation layer, the application layer) related to providing data to the application are referred to as the higher communication layers (HCL). The interface between LCL and HCL is referred to as communication service interface (CSIF).

3GPP network provides LCL of communication function (industrial radio communication) for distributed automation application system. Fieldbuses using serial communication (e.g., PROFIBUS DP, Modbus RTU, CC-Link, etc.) and Industrial Ethernet networks (e.g., EtherNet/IP, Modbus TCP, POWERLINK, EtherCAT, CC-Link IE Field, etc.) also provide LCL of communication function (industrial wired network communication). The TSN technology is used to support real-time control and synchronization of high-performance machines over a single, standard Ethernet network, supporting multi-vendor interoperability and integration. In order to enable seamless interoperability with existing wired networks, the 5G network needs to be end-to-end integrated into the industrial network control and management process using TSN.

The higher communication layers (HCL) can be provided by communication in automation technologies (e.g., OPC UA, PROFINET, etc.).

Annex C: Analysis of relationship between OPC UA and FF architecture

C.1 Overview

OPC 10000-1 [20] presents the concepts and overview of OPC UA. OPC UA is applicable to components in all industrial domains, such as industrial sensors and actuators, control systems, Manufacturing Execution Systems and Enterprise Resource Planning Systems, including the Industrial Internet of Things (IIoT), Machine To Machine (M2M) as well as Industrie 4.0. These systems are intended to exchange information and to use command and control for industrial processes. OPC UA defines a common infrastructure model to facilitate this information exchange by specifies the following:

- The information model to represent structure, behaviour and semantics.
- The message model to interact between applications.
- The communication model to transfer the data between end-points.

- The conformance model to guarantee interoperability between systems.

The OPC UA specifications are layered to isolate the core design from the underlying computing technology and network transport. This allows OPC UA to be mapped to future technologies as necessary, without negating the basic design. Mappings and data encodings are described in OPC 10000-6 [21]. Three data encodings are defined:

- XML/text
- UA Binary
- JSON

In addition, several protocols are defined:

- OPC UA TCP
- HTTPS
- WebSockets

The OPC UA systems architecture models Clients and Servers as interacting partners (Client Server model using TCP, HTTPS, WebSockets as transport protocols). OPC UA Client can send and receive OPC UA Service requests and responses to the OPC UA Server. OPC UA Client also can send publishing requests and receive notifications to the OPC UA Server. OPC UA Server to OPC UA Server interactions in the Client Server model are interactions in which one Server acts as a Client of another Server, it supports aggregation of data from lower-layer Servers and concentrator interfaces to Clients for single points of access to multiple underlying Servers. OPC UA Connection establishes a full duplex channel between a Client and Server by TCP/IP and WebSockets.A socket is the TransportConnection in the TCP/IP implementation. The URL scheme for endpoints using OPC UA TCP is "opc.tcp".

In addition to the Client Server model, OPC UA defines a mechanism for Publishers to transfer the information to Subscribers using the PubSub model which is described in OPC 10000-14 [22] (PubSub model using UDP, Ethernet, AMQP, MQTT as transport protocols). With PubSub, OPC UA Applications do not directly exchange requests and responses. Instead, Publishers send messages to a Message Oriented Middleware, without knowledge of what, if any, Subscribers there may be. Similarly, Subscribers express interest in specific types of data, and process messages that contain this data, without knowledge of what Publishers there are. Message Oriented Middleware is software or hardware infrastructure supporting sending and receiving messages between distributed systems.

To cover a large number of use cases, OPC UA PubSub supports two largely different Message Oriented Middleware variants. These are:

- A broker-less form, where the Message Oriented Middleware is the network infrastructure that is able to route datagram-based messages. Subscribers and Publishers use datagram protocols like UDP multicast.
- A broker-based form, where the Message Oriented Middleware is a Broker. Subscribers and Publishers use standard messaging protocols like AMQP or MQTT to communicate with the Broker. All messages are published to specific queues (e.g. topics, nodes) that the Broker exposes and Subscribers can listen to these queues. The Broker may translate messages from the formal messaging protocol of the Publisher to the formal messaging protocol of the Subscriber.

OPC UA covers the communication and information layer of reference architecture model for Industrie 4.0 which is defined in RAMI4.0 [23]. Specially, for communication in the field OPC UA now start to design to use UDP and specialized protocols like TSN or 5G for deterministic communication by PubSub extensions.

3GPP TS 22.104 [3] defines service requirements for vertical applications (e.g., mobile robots and augmented reality, etc.). 3GPP TS 22.263 [24] defines service requirements for video, imaging and audio for professional applications (VIAPA). The OPC UA information modelling framework turns data into information. OPC UA provides information models to support vertical applications (e.g., Robotics, Machine Vision, etc.)

Editor's Note: Relationship between OPC-UA and FFAPP is FFS.

Annex D (informative): Deployment Models

D.1 General

This clause describes some possible deployments of the functional model provided in clause 7.1.

In FF scenarios, there are different domains which need to be captured:

- **OT production domain**: the communications infrastructure on the factory premises used by real-time and non-real-time control systems. This may comprise both 3GPP (e.g. 5G NPN) and non-3GPP networks.
- **IT enterprise domain**: the communications infrastructure on the factory premises used for non-real-time resource planning and supervision. In this domain the management/provisiong of IIOT applications may be handled.
- **Service providers domain**: the communication infrastructure used for the purposes of network configuration, management and commissioning. This may be deployed by the factory operator or 3rd party service provider. MNO may also be part of the service providers domain, in scenarios when the factory uses private slices by the PLMN.

The enabler layer (FAE, SEAL layer) may be deployed as part of the different domains; this can be as part of the OT domain or PLMN/NPN operator domain, or at the FF application service provider domain (this can be at IT enterprise domain or service provider's domain), or at 3rd party service provider's domain.

Editor's Note: Here, for simplicity we assume that SEAL layer is co-located with FAE layer. However, FAE and SEAL may be in different domains (enhancement of SEAL deployment models for FF use cases is FFS).

D.2 FAE/SEAL Server deployment in PLMN/NPN operator domain

In this deployment, the enabler layer (FAE/SEAL server) resides at the NPN/PLMN operator domain and can be seen as PLMN/NPN-owned application entity which supports the exposure of northbound APIs to the IT enterprise / service providers domain (depending on where the application specific services are deployed). Also, with this deployment, the FAE / SEAL servers can support the the real-time interactions between the applications at the devices and the network side, e.g. for device communication management (e.g QoS).

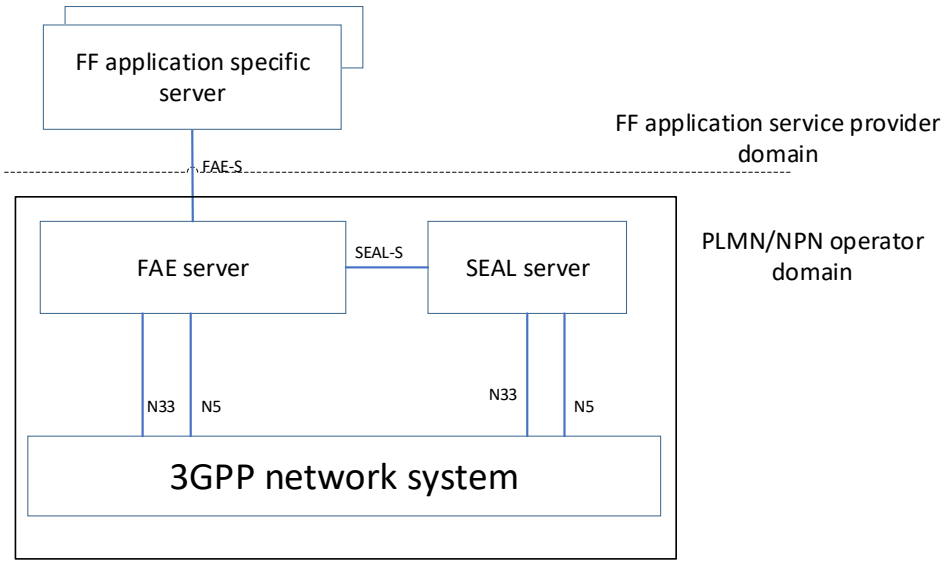

Figure D.2-1: FAE/SEAL Server at PLMN/NPN operator domain

Editor's Note: In this deployment, both single-PLMN/NPN and multi-PLMN/NPN deployment options may exist. It is FFS to further investigate deployments within PLMN/NPN domain, based on multi-PLMN and PLMN-NPN interactions.

D.3 FAE/SEAL Server deployment at FAE/SEAL service provider domain

In this deployment, the enabler layer (FAE/SEAL server) resides at the FAE/SEAL provider domain, on top of the 5G NPN (e.g. at IT enterprise domain). In this deployment, the FAE/SEAL layer supports the non-real-time resource planning and supervision of IIOT applications. One particular example may be the co-location of FAE/SEAL layer for supporting device management services (e.g. device provisioning, onboarding/offboarding, connectivity).

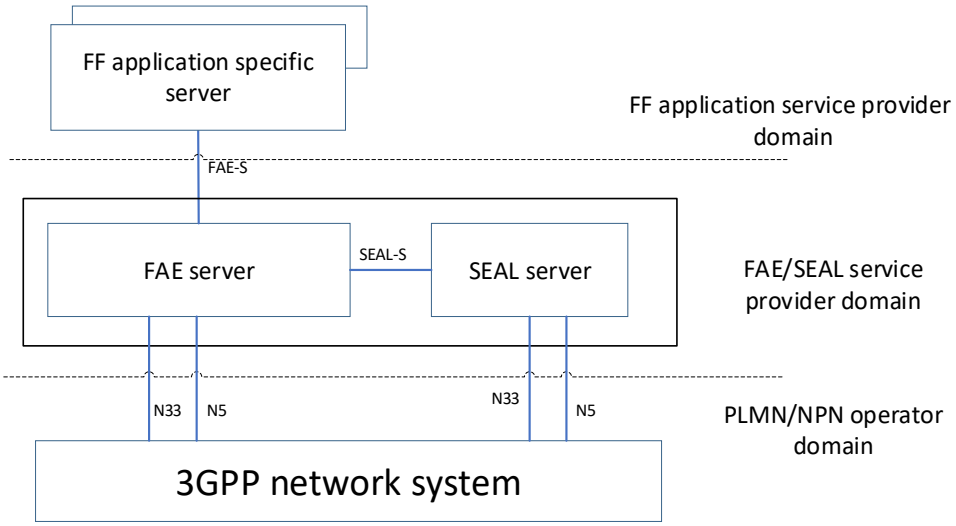

Figure D.3-1: FAE/SEAL Server at FAE/SEAL service provider domain

Editor's Note: It is FFS to further investigate centralized and distributed deployments within FAE/SEAL service provider domain.

D.4 FAE/SEAL Server deployment at FF application service provider domain

In this deployment, the enabler layer (FAE/SEAL server) resides at the FF application service provider's domain. The FAE/SEAL layer supports the control/influence of the network configuration, management and commissioning by the service provider.

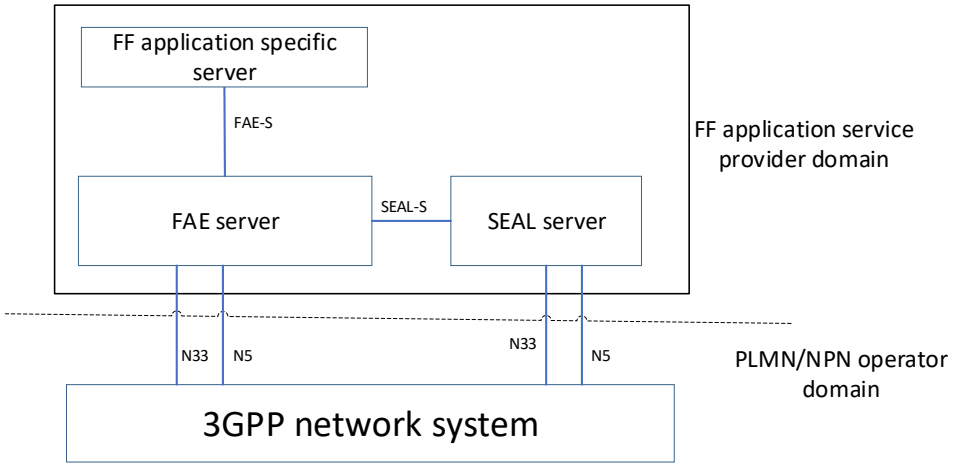

Figure D.4-1: FAE/SEAL Server at FF application service provider domain

Editor's Note: It is FFS to further investigate centralized and distributed deployments within FF application service provider domain.

Annex E: Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2019-01	SA6#28					TR skeleton	0.0.0
2019-01	SA6#28					Implementation of the following pCRs approved by SA6: S6-190292	0.1.0
2019-04	SA6#30					Implementation of the following pCRs approved by SA6: S6-190774, S6-190775, S6-190776, S6-190844, S6-190874, S6-190846	0.2.0
2019-05	SA6#31					Implementation of the following pCRs approved by SA6: S6-191254, S6-191240, S6-191243, S6-191255	0.3.0
2019-07	SA6#32					Implementation of the following pCRs approved by SA6: S6-191497, S6-191498, S6-191509	0.4.0
2019-09	SA6#33					Implementation of the following pCRs approved by SA6: S6-191918, S6-191921, S6-191995, S6-191996	0.5.0
2019-11	SA6#34					Implementation of the following pCRs approved by SA6: S6-192259, S6-192260, S6-192171, S6-192364, S6-192365, S6-192263	0.6.0
2020-01	SA6#35					Implementation of the following pCRs approved by SA6: S6-200251, S6-200309, S6-200253, S6-200311, S6-200335, S6-200142, S6-200258, S6-200316	0.7.0
2020-05	SA6#37-e					Implementation of the following pCRs approved by SA6: S6-200831, S6-200909, S6-200958, S6-200959, S6-200935, S6-200960, S6-200961, S6-200853	0.8.0
2020-07	SA6#38-e					Implementation of the following pCRs approved by SA6: S6-201171, S6-201221, S6-201250, S6-201095, S6-201252, S6-201251, S6-201210, S6-201253, S6-201254, S6-201255, S6-201256	0.9.0
2020-09	SA6#39-e					Implementation of the following pCRs approved by SA6: S6-201596, S6-201664, S6-201639, S6-201665, S6-201666, S6-201667, S6-201411	0.10.0
2020-09	SA#89-e	SP-200829				Presentation for information at SA#89-e	1.0.0
2020-10	SA6#39 BIS-e					Implementation of the following pCRs approved by SA6: S6-201841, S6-201953, S6-201937, S6-202014, S6-201926, S6-202015, S6-202016	1.1.0
2020-11	SA6#39 BIS-e					Re-implementation of S6-201953	1.1.1
2020-11	SA6#40-e					Implementation of the following pCRs approved by SA6: S6-202260, S6-202276, S6-202244, S6-202347, S6-202348, S6-202278, S6-202277, S6-202110, S6-202115	1.2.0
2021-02	SA6#41-e					Implementation of the following pCRs approved by SA6: S6-210259, S6-210274, S6-210364, S6-210260, S6-210365, S6-210262, S6-210366, S6-210367, S6-210264, S6-210368, S6-210036, S6-210266, S6-210171, S6-210038	1.3.0
2021-03	SA6#42-e					Implementation of the following pCRs approved by SA6: S6-210442, S6-210450, S6-210441, S6-210713, S6-210605, S6-210606, S6-210714, S6-210563, S6-210600, S6-210715, S6-210716	1.4.0
2021-04	SA6#42-bis-e					Implementation of the following pCRs approved by SA6: S6-210758, S6-210970, S6-210760, S6-210763, S6-210784, S6-210800, S6-210971, S6-211077, S6-211032, S6-210761, S6-210990, S6-210841, S6-211031, S6-210785, S6-210991, S6-210992, S6-210865, S6-211080	1.5.0
2021-06	SA6#43-e					Implementation of the following pCRs approved by SA6: S6-211378, S6-211161, S6-211179, S6-211395, S6-211491, S6-211397	1.6.0
2021-07	SA6#44-e					Implementation of the following pCRs approved by SA6: S6-211560, S6-211762, S6-211562, S6-211731, S6-211732, S6-211734, S6-211735, S6-211736, S6-211737, S6-211738, S6-211538, S6-211739, S6-211740, S6-211742, S6-211743, S6-211744, S6-211745, S6-211803	1.7.0
2021-09	SA#93-e	SP-210948				Presentation for approval at SA#93-e	2.0.0
2021-09	SA#93-e	SP-210948				MCC Editorial update for publication after TSG SA approval (SA#93)	17.0.0