ETSI TS 123 436 V19.5.0 (2026-04)

TECHNICAL SPECIFICATION

LTE;
5G;
Functional architecture and information flows for Application Data Analytics Enablement Service
(3GPP TS 23.436 version 19.5.0 Release 19)

Reference
RTS/TSGS-0623436vj50

Keywords
5G,LTE

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification 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.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

Introduction

Considering vertical-specific applications and edge applications as the major consumers of 3GPP-provided data analytics services, the application enablement layer can play role on the exposure of data analytics services from different 3GPP domains to the vertical/ASP in a unified manner; and on defining, at an overarching layer, value-add application data analytics services which cover stats/predictions for the end-to-end application service.

This technical specification provides procedures for enabling ADAE service over 3GPP networks, while the architecture is defined in TS 23.434 [2].

1 Scope

The present document specifies the procedures, information flows and APIs necessary for Application Data Analytics Enablement SEAL Service.

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 23.434: "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows".

[3] 3GPP TS 26.531: "Data Collection and Reporting; General Description and Architecture".

[4] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[5] 3GPP TS 28.104: "Management and orchestration; Management Data Analytics".

[6] 3GPP TS 23.435: "Procedures for Network Slice Capability Exposure for Application Layer Enablement Service".

[7] 3GPP TS 28.552: "Management and orchestration; 5G performance measurements".

[8] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs".

[9] 3GPP TS 23.501: “System architecture for the 5G System”.

[10] GSMA NG.116 - Generic Network Slice Template.

[11] 3GPP TS 22.261: “Service requirements for the 5G system”.

[12] 3GPP TS 28.545: "Management and orchestration; Fault Supervision (FS)".

[13] 3GPP TS 23.433: "Service Enabler Architecture Layer for Verticals (SEAL); Data Delivery enabler for vertical applications".

[14] 3GPP TS 23.558: "Architecture for enabling Edge Applications".

[15] 3GPP TS 28.623: "Telecommunication management; Generic Network Resource Model (NRM) Integration Reference Point (IRP); Solution Set (SS) definitions".

[16] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[17] 3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

[18] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[19] 3GPP TS 23.482: “Functional architecture and information flows for AIML Enablement Service”.

[20] 3GPP TS 33.434: "Security aspects of Service Enabler Architecture Layer (SEAL) for verticals".

3 Definitions of terms and abbreviations

3.1 Terms

For the purposes of the present document, the terms 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].

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].

ADAES	Application Data Analytics Enabler Server
ADAEC	Application Data Analytics Enabler Client
A-ADRF	Application layer - Analytical Data Repository Function
A-DCCF	Application layer - Data Collection and Coordination Function
ASP	Application Service Provider
DNAI	Data Network Access Identifier
EAS	Edge Application Server
EEL	Edge Enabler Layer
EES	Edge Enabler Server
FLS	Fused Location Server
LMS	Location Management Server
MDAS	Management Domain Analytics Service
NSCE	Network Slice Capability Enablement
NWDAF	Network Data Analytics Function
OAM	Operation, Administration and Maintenance
RNIS	Radio Network Information Service
RTT	Round-Trip Time
VAL	Vertical Application Layer

4 Architectural requirements

4.1 General Description

The following clauses specify the requirements for application data analytics enablement service.

4.2 General Requirements

[AR-4.2-a] The ADAE client and the ADAE server shall support one or more VAL applications.

[AR-4.2-b] Supported ADAE capabilities shall be offered as APIs to the VAL applications.

[AR-4.2-c] The ADAE shall support interaction with 3GPP network system to consume network and management data analytics services.

[AR-4.2-d] The ADAE client shall be capable to communicate with one or more ADAE servers of the same ADAE service provider.

4.3 ADAE internal architecture requirements

[AR-4.3-a] The ADAE layer shall be able to provide a data collection coordination functionality to enable the collection from diverse data sources (OAM, 5GC, UE) per application data analytics event type.

[AR-4.3-b] The ADAE layer shall include a data analytics repository function to store application data analytics.

[AR-4.3-c] The data collection coordination and repository capabilities may be offered as APIs to ADAE server.

4.4 ADAE capability related requirements

[AR-4.4-a] The ADAE server shall be capable of providing data analytics for the VAL server performance.

[AR-4.4-b] The ADAE server shall be capable of providing data analytics for the VAL application sessions (for both Uu-based and PC5-based sessions).

[AR-4.4-c] The ADAE server shall be able to collect application performance measurements and analytics from one or more ADAE clients.

[AR-4.4-d] The ADAE server shall be capable of collecting edge data from one or more edge platforms

[AR-4.4-e] The ADAE server shall enable the exposure of edge data analytics to the VAL applications

[AR-4.4-f] The ADAE server shall be capable of providing data analytics for the VAL server or VAL session performance for a requested slice or slice instance.

[AR-4.4-g] The ADAE server shall be capable of providing data analytics for the location accuracy of one or more VAL UEs.

[AR-4.4-h] The ADAE server shall be capable of providing data analytics related to the availability and status of one or more service APIs.

5 Application architecture for ADAES

5.1 General

This clause provides the functional architecture for ADAE. This includes the on-network and off-network functional models which are provided in detail in clause 5.2.

In addition, the ADAE internal architecture is described in 5.3, which aligns with the 3GPP data analytics framework (specified in TS 23.288 [4]) and introduces new logical entities within ADAE framework, such as the A-DCCF and A-ADRF.

5.2 Functional architecture

5.2.1 General

The functional architecture for the application data analytics enablement is based on the generic functional model specified in clause 6.2 of 3GPP TS 23.434 [2]. It is organized into functional entities to describe a functional architecture which addresses the support for application data analytics enablement aspects for vertical applications.

5.2.2 On-network Functional Architecture

For the on-network functional architecture, both service-based representation and reference point representation are provided.

Figure 5.2.2-1 depicts the application data analytics enablement architecture in the non-roaming case, using the reference point representation showing how various entities interact with each other.

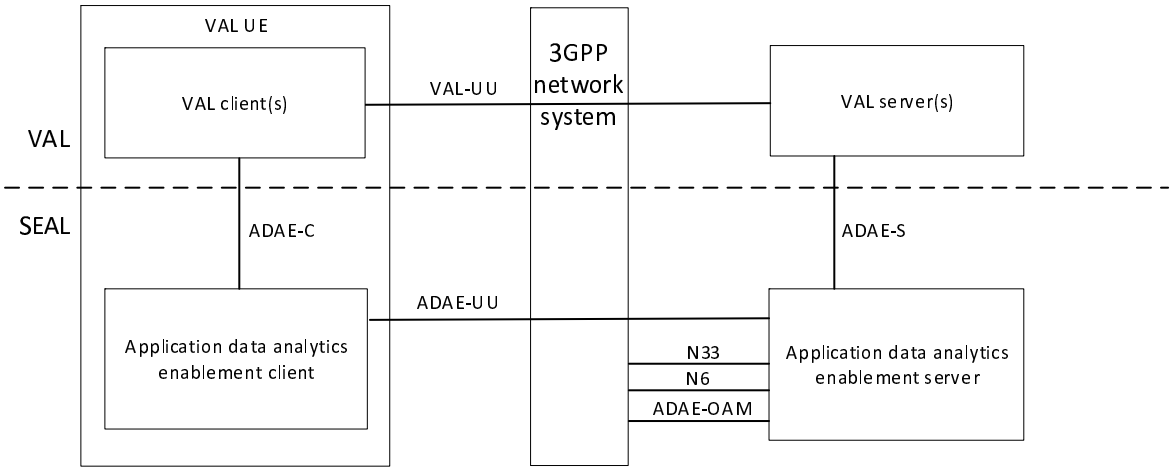

Figure 5.2.2-1: Architecture for application data analytics enablement – reference points representation

The application data analytics enablement client communicates with the application data analytics enablement server over the ADAE-UU reference point. The application data analytics enablement client provides the support for application data analytics enablement functions to the VAL client(s) over ADAE-C reference point. The VAL server(s) communicates with the application data analytics enablement server over the ADAE-S reference point. The application data analytics enablement server, acting as AF, may communicate with the 5G Core Network functions (over N33 reference point to NEF and N6 reference point to UPF) and OAM (over ADAE-OAM interface).

Figure 5.2.2-2 exhibits the service-based interfaces for providing and consuming application data analytics enablement services. The application data analytics enablement server could provide service to VAL server and ADAE client through interface SAdae.

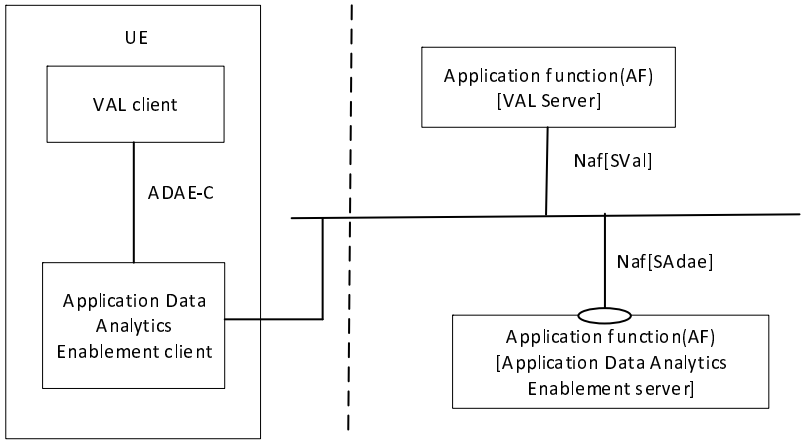

Figure 5.2.2-2: Architecture for application data analytics enablement – Service based representation

Figure 5.2.2-3 illustrates the service-based representation for utilization of the 5GS network services based on the 5GS SBA specified in 3GPP TS 23.501 [9].

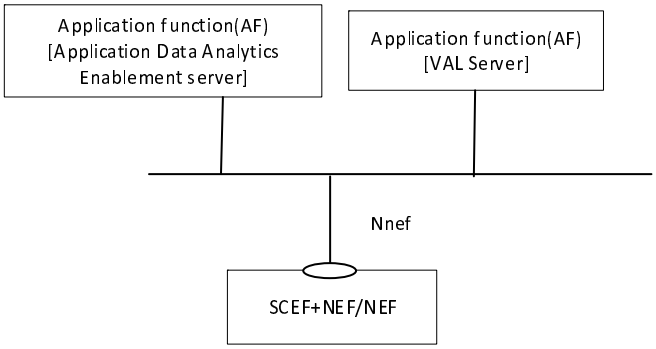

Figure 5.2.2-3: Architecture for application data analytics enablement utilizing the 5GS network services based on the 5GS SBA – Service based representation

Figure 5.2.2-4 illustrates the architecture for inter-service communication between ADAES server and other SEAL server.

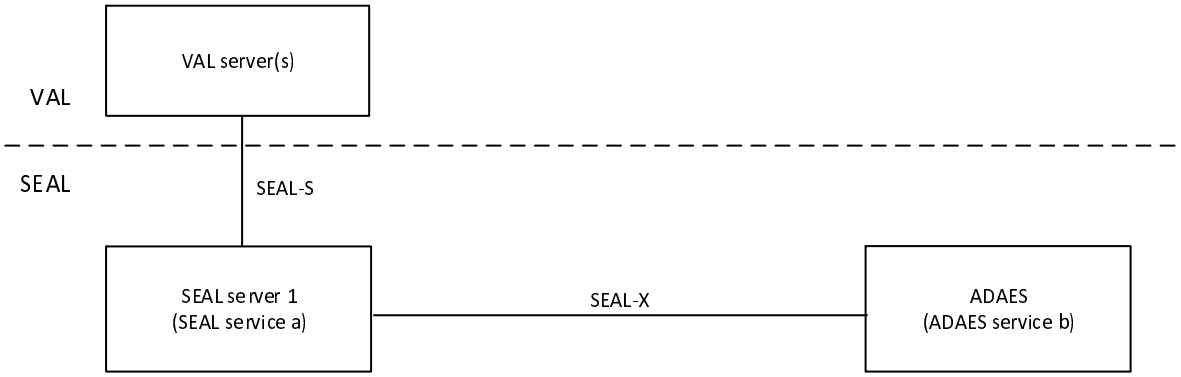

Figure 5.2.2-4: Inter-service communication between ADAES server and other SEAL server

The ADAE server interacts with another SEAL server for inter-service communication over SEAL-X reference point.

5.2.3 Off-network Functional Architecture

Figure 5.2.3-1 illustrates the generic off-network functional model for ADAE.

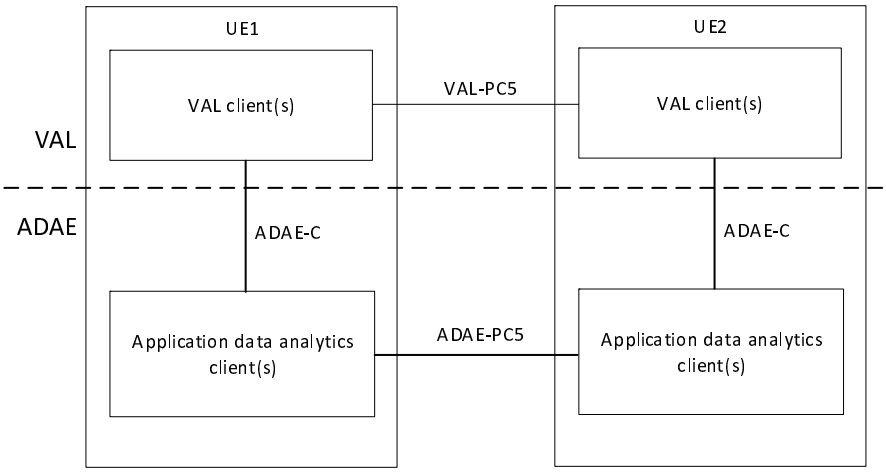

Figure 5.2.3-1: Generic off-network functional model

In the vertical application layer, the VAL client of UE1 communicates with VAL client of UE2 over VAL-PC5 reference point. An application data analytics enablement client of UE1 interacts with the corresponding application data analytics enablement client of UE2 over ADAE-PC5 reference points. The UE1, if connected to the network via

Uu reference point, can also act as a UE-to-network relay, to enable UE2 to access the VAL server(s) over the VAL-UU reference point.

The service-based interface representation is specified in clause 15 of 3GPP TS 23.434 [2].

5.2.4 Functional Architecture for supporting interactions with SEAL AIMLE

Figure 5.2.4-1 illustrates the architecture representation including AIMLE (as specified in 3GPP TS 23.482 [19]) for supporting ML-enabled analytics in ADAES. In this representation, the AIML support capabilities serve ADAES to enhance its analytics services. Based on the VAL request to provide ML-enabled analytics, ADAES may consume AIMLE services (e.g., for ML model training for a given analytics ID) to derive application layer data analytics.

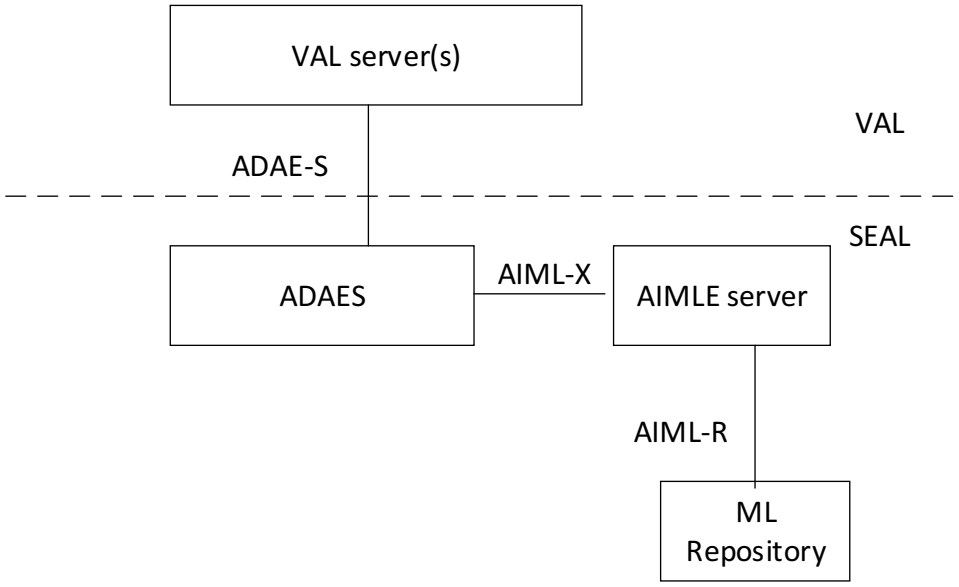

Figure 5.2.4-1: Architecture representation for supporting AIML-enabled ADAE analytics.

For the interaction between AIMLE server and ADAES, AIML-X is introduced to support consuming AIMLE services for deriving ADAE analytics (e.g. VAL server performance analytics).

The ML repository is specified in 3GPP TS 23.482 [19] as a repository for the ML model and registry for the ML-related information (such as ML/FL members). This repository may be utilized by ADAES via AIMLE server (via AIML-R) for fetching ML-related information (e.g., trained ML model, ML/FL members) which is used for a given ADAE analytics event.

Further details on the AIMLE capabilities and architecture, where the ADAES is a consumer of the AIMLE services, are specified in 3GPP TS 23.482 [19].

5.3 ADAE internal architecture

In ADAE framework, A-DCCF and A-ADRF can be defined as functionalities within the internal ADAE architecture and can offer the following functionalities:

- Application layer - Data Collection and Coordination Function (A-DCCF) coordinates the collection and distribution of data requested by the consumer (ADAE server). Data Collection Coordination is supported by a A-DCCF. ADAE server can send requests for data to the A-DCCF rather than directly to the Data Sources. A-DCCF may also perform data processing/abstraction and data preparation based on the VAL server requirements.

- Application layer – Analytics and Data Repository Function (A-ADRF) stores historical data and/or analytics, i.e., data and/or analytics related to past time period that has been obtained by the consumer (e.g. ADAE server). After the consumer obtains data and/or analytics, consumer may store historical data and/or analytics in an A-ADRF. Whether the consumer directly contacts the A-ADRF or goes via the A-DCCF is based on configuration.

Figure 5.3-1 illustrates the generic functional model for ADAE when re-using the 3GPP network data analytics model.

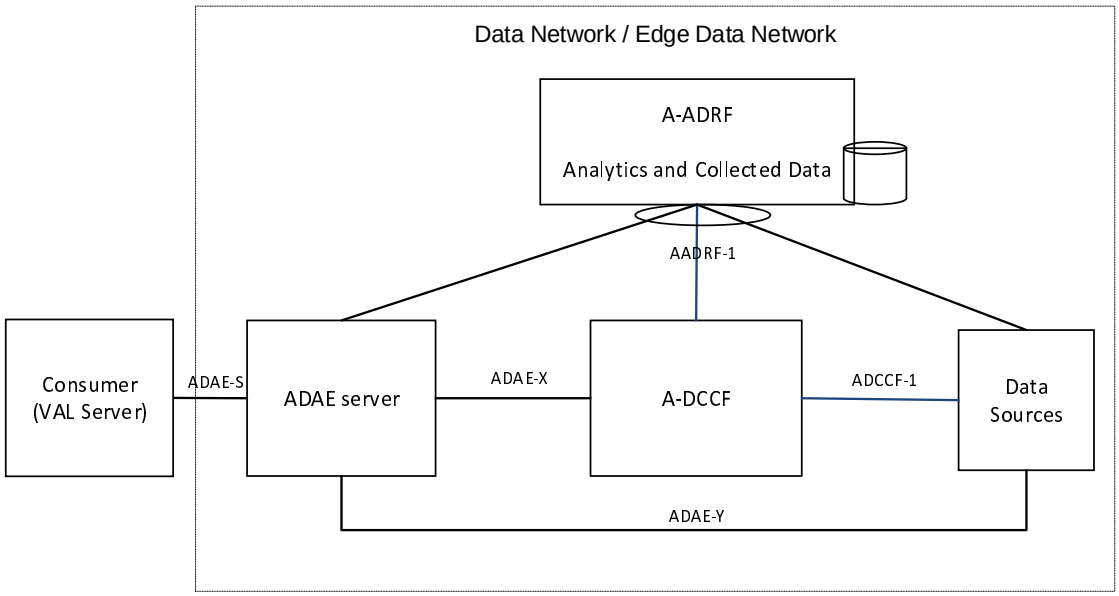

Figure 5.3-1: ADAE internal functional architecture

In this model, an A-DCCF is used to fetch data or put data into an application-level entity (e.g. A-ADRF, Data Source). Such A-DCCF coordinates the collection and distribution of data requested by ADAE server (over ADCCF-1, ADAE-X). ADAE server can also directly interact with the Data Sources via ADAE-Y.

Also, Application layer – Analytics and Data Repository Function (A-ADRF) can be used to store historical data and/or analytics, i.e., data and/or analytics related to past time period that has been obtained by the ADAE server (via AADRF-1) or other NFs/NWDAF. ADAE server can also fetch historical data from A-ADRF. Whether the ADAE server directly contacts the A-ADRF or goes via the A-DCCF is based on configuration.

Data Sources can be 5GS data sources (5GC, OAM) or enablement layer data sources (SEAL, EEL) or external data sources at the DN side (VAL server/ EAS) and VAL UEs. A-DCCF and A-ADRF can be used only for interacting with certain data sources (e.g., 5GC, OAM) based on configuration, and can be hidden from the VAL layer.

NOTE: If the Data Source is the VAL UE, then the data collection mechanism shall reuse the SA4 mechanism based on EVEX study (TS 26.531 [3]).

5.4 Functional entities description

5.4.1 General

The functional entities for ADAE service are described in the following subclauses.

5.4.2 Application Data Analytics Enablement client

The application data analytics enablement and provides client side functionalities for the functionalties provided by the application data analytics enablement server. The application data analytics enablement client interacts with the application data analytics enablement server.

5.4.3 Application Data Analytics Enablement server

The application data analytics enablement server functional entity provides application layer analytics to support the VAL applications. The application data analytics enablement server acts as CAPIF's API exposing function as specified in 3GPP TS 23.222 [8]. The application data analytics enablement server also supports interactions with the corresponding application data analytics enablement server in distributed SEAL deployments. The ADAE server also interacts with 3GPP core network over N33 or N6 interface to subscribe to changes in configuration or other application server specific events. The ADAE server also acts as a co-ordinating entity to collect data from different sources and perform necessary actions to provide required analytics.

The ADAE server provides following server side functionalities:

- monitoring performance of an application (VAL server or EAS, application session) and providing support for application performance analytics;
- monitoring performance of a given network slice (from a list of subscribed slices for the VAL customer) and also usage pattern, and providing support for slice-specific application performance analytics and slice usage pattern analytics;
- monitoring performance of an application session among two or more VAL UEs within a service or group, and providing support for UE-to-UE application performance analytics;
- monitoring accuracy of a location and providing support for location accuracy analytics;
- monitoring availability and service level for service APIs and providing support for service API analytics;
- monitoring edge load parameters and providing support for edge load analytics;
- monitoring ranging/SL positioning data and location information, and providing support for collision detection analytics.
- monitoring location information and providing support for location-related UE group analytics.
- monitoring application layer AI/ML member capability data and providing support for Application Layer AI/ML Member Capability Analytics.

To support ML-enabled analytics services, the ADAE server may provide the above server-side functionalities by consuming SEAL AIMLE services (as specified in 3GPP TS 23.482 [19]).

5.5 Reference points description

5.5.1 General

The reference points for the functional model for application data analytics enablement are described in the following subclauses.

5.5.2 ADAE-UU

The interactions related to application data analytics enablement functions between the application data analytics enablement client and the application data analytics enablement server are supported by ADAE-UU reference point. This reference point utilizes Uu reference point as described in 3GPP TS 23.401 [16] and 3GPP TS 23.501 [9].

5.5.3 ADAE-PC5

The interactions related to application data analytics enablement functions between the application data analytics enablement clients located in different VAL UEs are supported by the ADAE-PC5 reference point. This reference point utilizes PC5 reference point as described in 3GPP TS 23.303 [17].

5.5.4 ADAE-C

The interactions related to application data analytics enablement functions between the VAL client(s) and the application data analytics enablement client within a VAL UE are supported by the ADAE-C reference point.

5.5.5 ADAE-S

The interactions related to application data analytics enablement functions between the VAL server(s) and the application data analytics enablement server are supported by the ADAE-S reference point. This reference point is an instance of CAPIF-2 reference point as specified in 3GPP TS 23.222 [8].

5.5.4 ADAE-X

The interactions related to application data analytics enablement functions between the application data analytics enablement server and the Application-layer DCCF (A-DCCF) for data coordination aspects are supported by the ADAE-X reference point.

5.5.5 ADAE-Y

The interactions related to application data analytics enablement functions between the application data analytics enablement server and the data producers (or data sources) for collecting data to be used for the ADAE analytics services (if A-DCCF is not used) are supported by the ADAE-Y reference point.

5.5.6 ADCCF-1

The interactions related to application data analytics enablement functions between the application layer data collection and coordination entity and the data sources for data coordination aspects are supported by the ADCCF-1 reference point.

5.5.7 AADRF-1

The interactions related to application data analytics enablement functions between the application data analytics enablement server (or the A-DCCF) and the application layer - analytics and data repository function (A-ADRF) for storing data and analytics related to the ADAE analytics services (if A-DCCF is not used) are supported by the AADRF-1 reference point.

5.5.8 SEAL-X

The interactions between the NSCE servers and other SEAL servers are generically referred to as SEAL-X reference point. The specific SEAL server interactions corresponding to SEAL-X are described in 3GPP TS 23.434 [2].

5.5.9 AIML-X

The interactions between the SEAL AIMLE server and ADAES for supporting ML-enabled analytics is generically referred to as AIML-X reference point. AIML-X is an instance of SEAL-X as described 3GPP TS 23.434 [2].

6 ADAE layer Functional Description

6.1 Support for application performance analytics

This feature supports the derivation and exposure of application layer analytics to provide insight on the operation and performance of an application (VAL server or EAS, application session), and in particular statistics or prediction on parameters related to e.g. VAL server number of connections for a given time and area, VAL server rate of connection requests, connection probability failure rates, RTT and deviations for a VAL server or VAL UE session, packet loss

rates etc. This feature also supports the collection of service experience information from the ADAE clients (as described in clause 8.9) to support application performance analytics.

6.2 Support for slice-specific application performance analytics

This feature introduces application layer analytics to provide insight on the performance of the VAL applications when using a given network slice (from a list of subscribed slices for the VAL customer). Such capability provides an analytics service to a consumer who can be either the VAL server (for helping to identify what slice it will use for its applications) or for other consumers such as SEAL NSCE to support on providing analytics (since NSCE doesn't contain an analytics engine for providing analytics on top of NWDAF [4] /MDAS [5]).

6.3 Support for UE-to-UE application performance analytics

This feature supports the derivation and exposure of application layer analytics to predict the performance of an application session among two or more VAL UEs within a service or group. Such prediction relates to application QoS attributes prediction for a given time horizon and area. This can be requested by the VAL server during the session, or the VAL server can subscribe to receive predicted application QoS downgrade indication for an ongoing session. Such analytics will help improving the application service experience and allow the VAL layer to pro-actively adapt to predicted application QoS changes.

6.4 Support for location accuracy analytics

This feature supports application layer analytics enablement to allow a VAL server to be notified based on analytics whether the accuracy of a location can be met for a given application and optionally for a given UE/group route. For example, a VAL server may request the ADAE server to provide analytics whether the accuracy of a location for the UEs within a VAL application is predicted to be sustainable or is expected to downgrade in a specific area or for an expected route from location A to location B.

6.5 Support for service API analytics

This feature introduces service API analytics to allow a VAL server or any other consumer (e.g. API provider) to be notified on the predicted /statistic availability and service level for the requested service API analytics. Such analytics may be utilized by the API provider to perform actions to avoid service API invocation failures or other actions like throttling/rate limitations. Also, such analytics will support the VAL server to identify if/when to perform an API invocation request based on the API expected status at the given area and time horizon.

6.6 Slice usage pattern analytics

Slice usage pattern analytics provides network slice usage pattern analytics based on collected network slice performance and analytics, historical network slice status, and network performance to help the analytics consumer manage the network slice.

6.7 Support for edge load analytics

Edge load analytics provide insight on the operation and performance of an EDN and in particular statistics or prediction on parameters related to:

- the EAS / EES load for one or more EAS/EES
- edge platform load parameters, which include the aggregated load per EDN or per DNAI due to the edge support services and e.g., load level of edge computational resources.

Such analytics can improve edge support services by allowing the pro-active edge service operation changes to deal with possible edge overload scenarios. For example, this can trigger EAS migration to a different EDN / central DN, or pro-active EAS reselection for a target UE or group of UEs.

6.8 Edge computing preparation analytics

This feature introduces exposure of edge computing preparation analytics of the EAS, EES, and/or ECS to the analytics consumer (e.g., the VAL server, ECS, EES). The ADAE server provides the edge computing preparation analytics based on collected edge deployment time information, historical edge computing preparation analytics, instantiation triggering time and registration time from the EDN.

6.9 Support for server-to-server performance analytics

This feature supports server-to-server performance analytics to allow an analytics consumer (such as VAL server or EES) to be notified on QoS analytics or predictions between two or more servers. Such prediction relates to QoS attributes prediction for a given time horizon and area. Such analytics allow the VAL layer to pro-actively adapt to predicted QoS changes.

6.10 Support for collision detection analytics

This feature supports collision detection analytics to allow an analytics consumer (such as VAL Server, LM server, UAE server, UAS application specific server) to be notified on analytics for collision detection between any target VAL UEs, collision detection between any UEs and target VAL UEs, or collision detection between any UE within the Area of Interest.

6.11 Support for location-related UE group analytics

This feature supports location-related UE group analytics to allow an analytics consumer (such as LMS) to be notified on analytics for UE group route or UE group member deviation. Such analytics can be used, e.g. UE group route prediction can be used to formulate application group profile with Expected Group Geographical Service Area as described in 3GPP TS 23.558 [14] clause 8.2.11. UE group member deviation prediction can be used for VAL to know which UE group member falls behind other group members or target group member (then VAL can send warning/reminder to the group members).

6.12 Support for Application Layer AI/ML Member Capability Analytics

This feature supports Application Layer AI/ML Member Capability Analytics to allow an analytics consumer (such as e.g. VAL Server, AIMLE Server) to be notified on analytics for application layer AI/ML Member capability. Such analytics can be used to support application layer AI/ML services, e.g. supporting FL member selection and reselection.

6.13 Support for VAL performance analytics for tethered UEs

This feature supports a new ADAES analytics functionality on tethered VAL connectivity performance. The tethered VAL connectivity performance can be defined as the application session performance corresponding to either only the tethered link (tethered UE and host UE) or the end-to-end VAL performance including the tethered link (as extension of VAL session performance analytics).

6.14 Support for DN Energy Analytics

This feature supports a logical functionality at the ADAES to provide analytics on the energy consumption /efficiency of an edge platform (including the EESs / EASs). The DN energy analytics is performed per DNN/ DNAI and may be used to trigger the application server migration to different cloud. The analytics are based on NWDAF analytics and UPF/DN measurements on user plane load as well as edge/app side measurements on the energy consumption.

6.15 Support for ML Model Performance Degradation Detection

This feature supports ML model performance degradation detection to allow a consumer (such as e.g. AIMLE Server) to be notified on performance degradation of an ML model. Such detection can be used to support application layer AI/ML operations, e.g. supporting decision making on retrain an ML model.

7 Identities and commonly used values

7.1 General

The common identities for SEAL refer to TS 23.434[2]. The following clauses list the additional identities and commonly used values for Application Data Analytics Enablement Service.

7.2 ADAE Server ID

The ADAE server ID uniquely identifies the application data analytics enablement server, and each ADAE server ID is unique within PLMN domain.

7.3 ADAE client ID

The ADAE client ID uniquely identifies the application data analytics enablement client.

7.4 A-ADRF ID

The A-ADRF ID uniquely identifies the application data analytics repository function.

7.5 A-DCCF ID

The A-DCCF ID uniquely identifies the application data collection and coordination function.

7.6 Data Producer ID

The Data Producer ID uniquely identifies the data producer / source which is used as input for application data analytics enablement services. Data Producer based on the analytics event, can be either a network function or a management domain function/service or an application server or client or an edge / cloud service.

7.7 ADAE service area

The ADAE service area is the area where the Application Data Analytics Enablement server owner provides its analytics services. It is equal to the coverage area for which analytics apply.

The ADAE service area can be expressed as a Topological Service Area (e.g. a list of TA), a Geographical Service Area (e.g. geographical coordinates) or both.

7.8 Analytics ID

The analytics ID (or analytics event ID) identifies the application layer analytics event which corresponds to the specified ADAE analytics services.

8 Procedures and information flows

8.1 General

This clause describes the procedures and the information flows related to the ADAE capabilities, as introduced in clause 6.

The security aspects for the ADAE services are specified in 3GPP TS 33.434 [20].

8.2 Procedure on support for application performance analytics

8.2.1 General

In this functionality, two procedures are described in more detail in clause 8.2.2 and 8.2.3 accordingly:

- one procedure for VAL server related analytics where an example in provided for VAL server performance,
- one procedure for VAL session/UE related analytics.

8.2.2 Procedure on VAL server performance analytics

Figure 8.2.2-1 illustrates the procedure where the VAL server performance analytics are performed based on data collected from the ongoing VAL sessions as well as data from the DN (VAL server, DN database or networking stack at the DN).

Pre-conditions:

1. ADAE Client (ADAEC) is connected to ADAES.
2. Data producers (e.g. A-ADRF, VAL Client) may be pre-configured with data producer profiles for the data they can provide. ADAES and ADAEC have discovered available data producers and their data producer profiles.

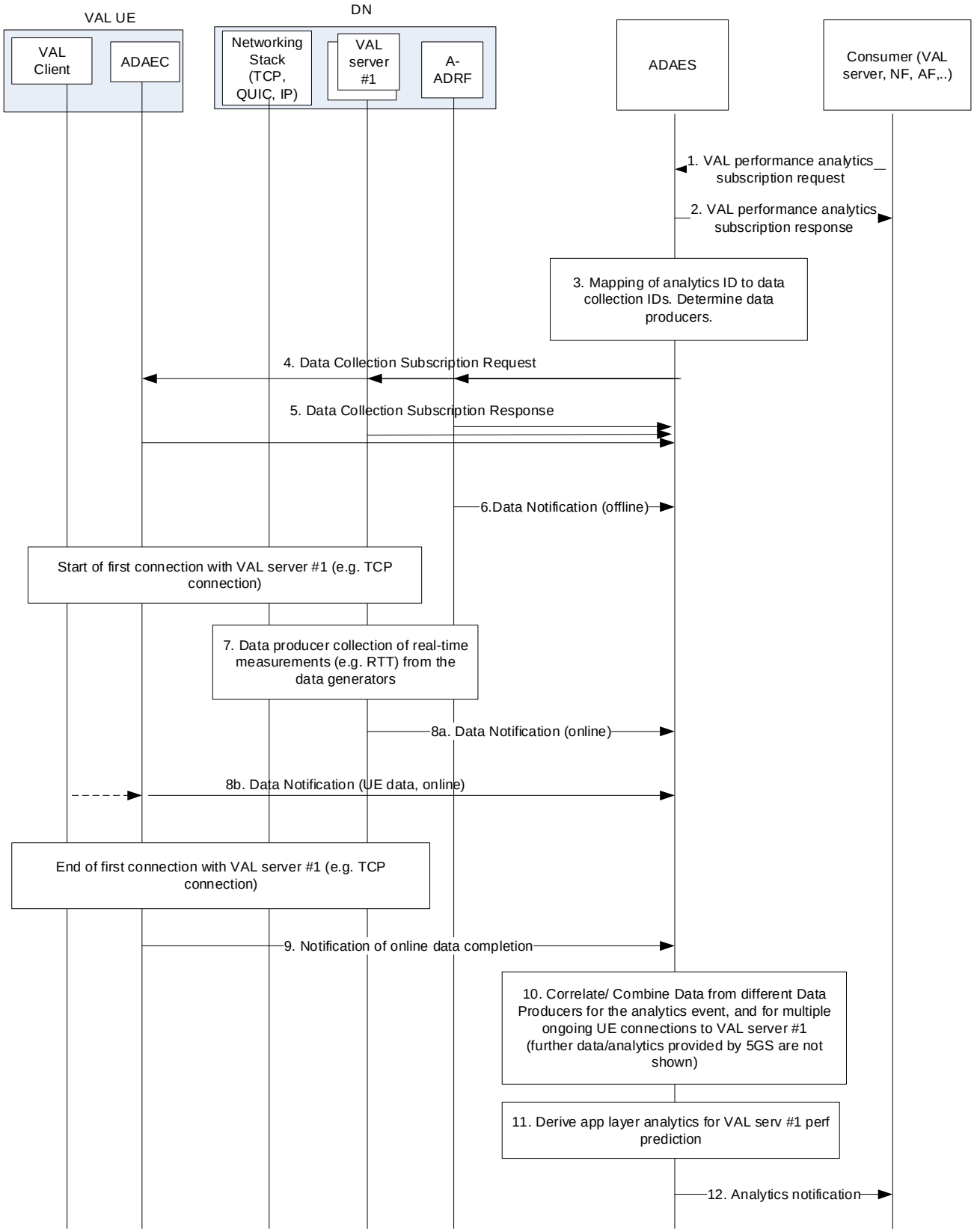

Figure 8.2.2-1: ADAES support for VAL server performance analytics

1. The consumer of the ADAES analytics service sends a VAL performance analytics subscription request to ADAES and provides the analytics event ID e.g. "VAL server performance analytics".

2. The ADAES sends a subscription response as a positive or negative acknowledgement to the consumer of the analytics service.

3. The ADAES maps the analytics event ID to a list of data collection event identifiers, and a list of data producer IDs. Such mapping may be preconfigured by OAM or may be determined by ADAES based on the analytics event type / vertical type and/or data producer profile.

4. The ADAES sends a data collection subscription request to the Data Producers (at the DN side or UE side) with the respective Data Collection Event ID and the requirement for data collection. Such data producers include the A-ADRF, the A-DCCF, the VAL server, SEALDD server, or the VAL UEs.

5. The Data Producer(s) sends a subscription response as a positive or negative acknowledgement to the ADAES.

NOTE: The ADAES acting as AF may also subscribe to NEF/SMF/PCF/NWDAF to monitor network/UE situation or network data analytics required for the application data analytics event.

6. The ADAES based on subscription, may receive offline stats/data from A-ADRF on the VAL server performance based on the analytics/data collection event ID. Such offline data can be average/peak throughput, average/maximum e2e delay, jitter, average application layer PER, availability, VAL server load, number of failed transactions, and can be for a given area and time of the day (based on the time/area of the request).

A session starts between the VAL server #1 and a UE (this could happen for more than one UEs).

7. The Data Producer at DN side, starts collecting data from the data generating entities, e.g. real-time networking or application data (from networking start at DN or VAL server itself), such as RTT, application layer PER, throughput.

8a. The Data Producer sends the real-time data to the ADAES, where the data correspond to the data collection ID or the analytics event ID for which the ADAES subscribed.

8b. The ADAES may receive also data (periodically or if a threshold is reached based on configuration) from the application of the UE within the ongoing session (via ADAEC). Such data can be about the RTT, average/peak throughput, jitter, QoE measurements (MOS, stalling events, stalling ratios, etc), QoS profile load, VAL server load, etc.

9. When the VAL UE session with VAL server finishes, the ADAEC notifies the ADAES of the completion of the reporting.

10. The ADAES abstracts or correlates the data based on the analytics event and the data collection configuration. Such correlation can be filtering of data for the same metrics but with different granularities or be combining/aggregating the data of segments of the end-to-end path (end to end is between VAL client and server). The outcome is an abstracted/correlated/filtered set of data.

11. The ADAES derives application layer analytics on VAL server #1 performance, based on the analytics ID and type of request. Such analytics can be stats or prediction for a given area/time and based on the event type for a given network configuration.

12. The ADAES sends the analytics to the consumer, where these analytics include the VAL server #1 predicted or statistic performance for a given area and time horizon, including also the confidence level.

NOTE: If the Data Producer in steps 4-5 and 8a is SEALDD server, procedure in clause 9.7.2.1 of 3GPP TS 23.433 [13] is used for the collection of the E2E transmission quality measurement results to ADAES.

8.2.3 Procedure on VAL session performance analytics

Figure 8.2.3-1 illustrates the procedure where the VAL session performance analytics are performed based on data collected from the ongoing VAL sessions.

Pre-conditions:

1. ADAEC is connected to ADAES.

2. Data producers (e.g. A-ADRF, VAL Client) may be pre-configured with data producer profiles for the data they can provide. ADAES and ADAEC have discovered available data producers and their data producer profiles.

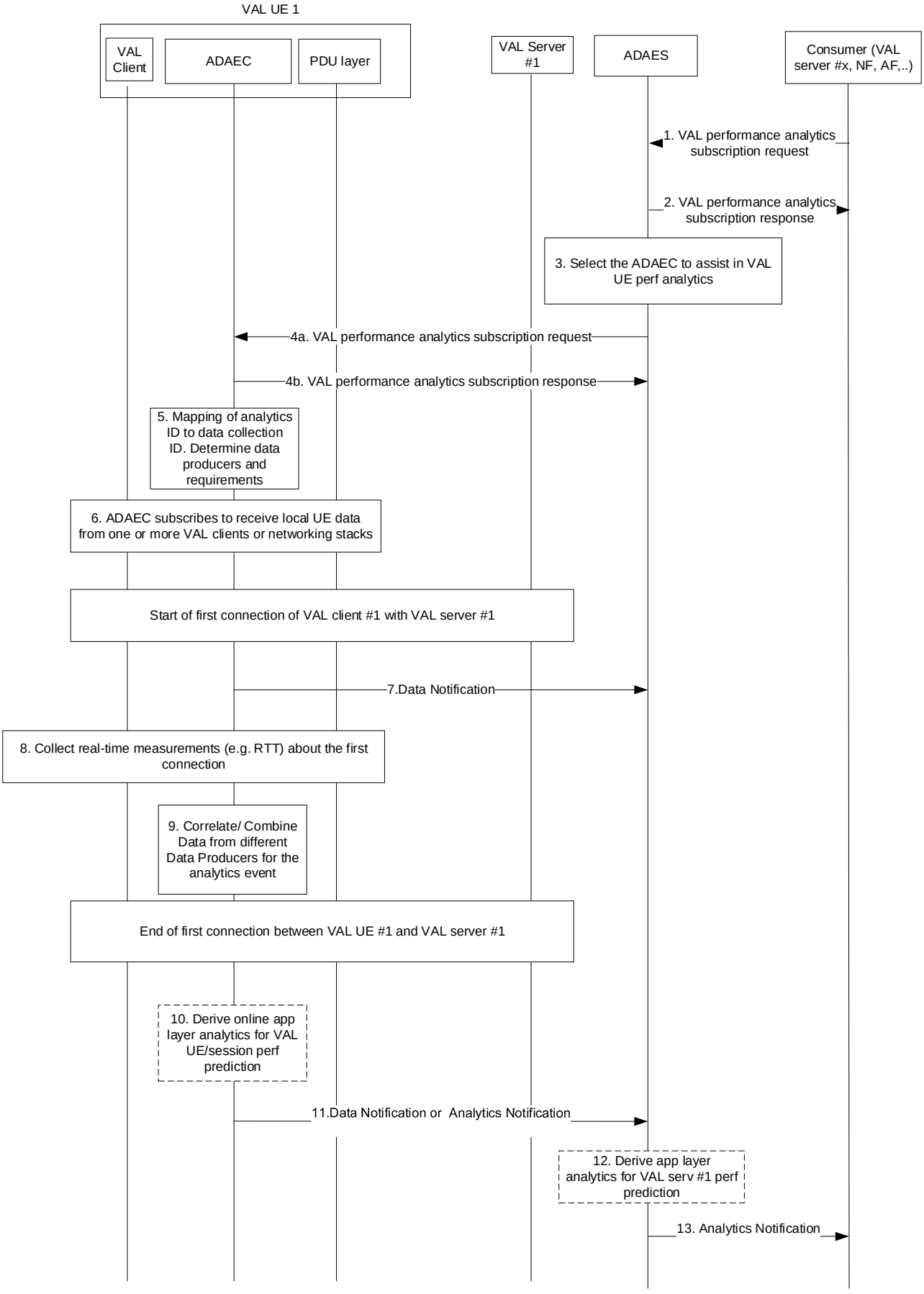

Figure 8.2.3-1: ADAES support for VAL session performance analytics

1. The consumer of the ADAES analytics service sends a VAL performance analytics subscription request to ADAES and provides the analytics event ID e.g. "VAL session performance analytics", the target VAL UE ID, VAL server ID/VAL application ID, the time validity and area of the request, the required confidence level, exposure level for providing UE analytics. If the consumer is the VAL server, the VAL server can provide to ADAEC application data related to the UE expected route/trajectory and VAL application traffic schedule / expected session time.

2. The ADAES sends a subscription response as an ACK to the consumer.

3. The ADAES selects the corresponding ADAEC of the VAL UE for which the local analytics need to be performed.

4a. The ADAES sends a subscription request to the ADAEC with the analytics event ID and the configuration of the reporting required (e.g., periodic, based on event with threshold).

4b. The ADAEC sends a subscription response to ADAES.

5. The ADAEC maps the analytics event ID to a list of data collection event identifiers or data collected IDs at the VAL UE or other UEs within the service and in proximity (in group-based communications). The ADAEC also determines the data producers using the analytics event ID, target data producer profile and optional preconfigured policies.

6. The ADAEC subscribes to the VAL clients and/or requests UE local data based on the respective Data Collection Event ID (or the analytics event ID if they already know the mapping). This data may come from the PDU layer of the UE (via listening the traffic), or via VAL client of one or more UEs (if an application consists of a group of UEs).

A session starts between the VAL UE #1 and a VAL server.

7. The ADAEC (after being aware from the VAL client that the session started) sends a notification to ADAES that a session started, and it could be possible to provide real-time data analytics for VAL UE performance in the target area.

8. The ADAEC starts collecting data from the corresponding data producers based on subscription. Such data can be about the RTT, throughput, jitter, QoE measurements, QoS profile load, etc. It can be also possible that VAL client provides to ADAEC application data related to the UE expected route/trajectory and VAL application traffic schedule / expected session time.

9. The ADAEC filters or correlates the data based on the analytics event and the data collection configuration.

10. When the VAL UE session finishes, the ADAEC (optionally) derives VAL session analytics to ADAES on VAL UE #1 performance, based on the analytics ID and type of request. Such analytics (if performed at the ADAEC can be stats or predictions on the RTT or RTT deviation, average/peak throughput, jitter, QoE measurements (MOS, stalling events, buffer related events), QoS profile load, VAL application traffic load etc. In case of prediction, a confidence level shall be also present and a time horizon for the predicted parameters.

11. The ADAEC sends the data of step 9 or the analytics of step 10 (if ADAEC performs analytics) to the ADAES.

12. The ADAES derives application layer analytics on VAL session performance (based on the data or analytics received by the ADAEC), based on the analytics ID and type of request. Such analytics can be stats or prediction for a given area/time and based on the event type for a given network configuration. Such analytics (if no analytics is performed at ADAEC) at ADAES can be stats or predictions on the RTT or RTT deviation, average/peak throughput, jitter, QoE measurements, QoS profile load, VAL application traffic load etc. In case of prediction, a confidence level shall be also present and a time horizon for the predicted parameters.

13. The ADAES sends the analytics to the consumer, where these analytics include the VAL UE #1 session predicted or statistic performance for a given area and time horizon, including also the confidence level.

8.2.4 Information flows

8.2.4.1 General

The following information flows are specified for VAL performance analytics based on 8.2.2 and 8.2.3.

8.2.4.2 VAL performance analytics subscription request

Table 8.2.4.2-1 describes information elements for the VAL performance analytics subscription request from the consumer (e.g. VAL server, NF, AF) to the ADAE server or from ADAE server to ADAE client.

Table 8.2.4.2-1: VAL performance analytics subscription request

Information element	Status	Description
Consumer ID	M	The identifier of the analytics consumer.
Analytics ID	M	The identifier of the analytics event. This ID can be for example “VAL server performance analytics” for procedure in 8.2.2, or “VAL session performance analytics” for procedure in 8.2.3.
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions.
VAL service ID	M	The identifier of the VAL service for which analytics subscription applies.
Target VAL UE ID(s)	O	The VAL UE identifier(s) for which the analytics subscription applies.
Target VAL server ID	O	If consumer is different from the VAL server, this identifier shows the target VAL server for which the analytics subscription applies (for procedure in 8.2.2).
Target data producer profile criteria	O	Characteristics of the data producers to be used.
ADAE client application data	O	Represent ADAE client application data (e.g. related to the UE expected route/trajectory and VAL application traffic schedule/expected session time) that the consumer can provide, if the consumer is VAL server.
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction).
Area of Interest	O	The geographical or service area for which the subscription request applies.
Time validity	O	The time validity of the subscription request.
Exposure level requirement	O	The level of exposure requirement (e.g. condition on providing UE analytics like threshold is reached) for the UE analytics to be exposed.
Reporting requirements	O	It describes the requirements for analytics reporting. This requirement may include e.g. the type and frequency of reporting (periodic or event triggered), the reporting periodicity in case of periodic, and reporting thresholds in case of event triggered.

8.2.4.3 VAL performance analytics subscription response

Table 8.2.4.3-1 describes information elements for the VAL performance analytics subscription response from the ADAE server to the consumer (e.g. VAL server, NF, AF) or from ADAE client to ADAE server.

Table 8.2.4.3-1: VAL performance analytics subscription response

Information element	Status	Description
Result	M	The result of the analytics subscription request (positive or negative acknowledgement).

8.2.4.4 Data collection subscription request

Table 8.2.4.4-1 describes information elements for the Data collection subscription request from the ADAE server to the Data Producer (e.g., A-DCCF, A-ADRF, VAL server, SEALDD server, or VAL UE via ADAE client).

Table 8.2.4.4-1: Data collection subscription request

Information element	Status	Description
ADAE server ID	M	The identifier of the ADAE server.
Data Collection Event ID	M	The identifier of the data collection event.
Data Collection requirements	M	The requirements for data collection, including the format of data, frequency of reporting, level of abstraction of data, level of accuracy of data.
Analytics ID	O	The identifier of the analytics event, for which the data collection is needed.
List of Data Producer IDs	O	In case when this request is performed via A-DCCF, then the list of Data Producer IDs is needed.
Target VAL UE ID(s) and address(es)	O	The VAL UE identifier(s) and IP address(es) for which the data collection subscription applies.
Target VAL server ID	O	This identifier shows the target VAL server for which the data collection subscription applies.
Target data producer profile criteria	O	Characteristics of the data producers to be used.
Area of Interest	O	The geographical or service area for which the requirement request applies.
Interest time period	O	Interested time period for which the requirement request applies (e.g. time of the day).
Time validity	O	The time validity of the request

8.2.4.5 Data collection subscription response

Table 8.2.4.5-1 describes information elements for the Data collection subscription response from the Data Producer (e.g., A-DCCF, A-ADRF, VAL server, SEALDD server, or VAL UE via ADAE client) to the ADAE server.

Table 8.2.4.5-1: Data collection subscription response

Information element	Status	Description
Result	M	The result of the data collection subscription request (positive or negative acknowledgement).

8.2.4.6 Data Notification

Table 8.2.4.6-1 describes information elements for the Data Notification from the Data Producer to the ADAE server.

Table 8.2.4.6-1: Data notification

Information element	Status	Description
Data Collection Event ID	M	The identifier of the data collection event.
Target VAL UE ID and address(es)	M (NOTE)	The VAL UE identifier(s) and IP address(es) for which the data apply.
Target VAL server ID	M (NOTE)	This identifier of the target VAL server for which the data applies.
Analytics ID	O	The identifier of the analytics event. This ID can be for example “VAL server performance analytics” for procedure in 8.2.2, or “VAL session performance analytics” for procedure in 8.2.3.
Data Type	O	The type of reported data samples which can be UE data, network data, application data, edge data, or different granularities / abstraction of data (e.g. real time, non real time).
Data Output	M	The reported data, which can be inform of measurements or offline/historical data on the requested parameter based on subscription. For example: - offline stats/data from A-ADRF on the VAL server performance based on the analytics/data collection event ID. Such offline data can be average/peak throughput, average/maximum e2e delay, jitter, average application layer PER, availability, VAL server load, number of failed transactions, and can be for a given area and time of the day (based on the time/area of the request). - from the application of the UE within the ongoing session (via ADAEC). Such data can be about the RTT, average/peak throughput, jitter, QoE measurements (MOS, stalling events, stalling ratios, etc), QoS profile load, VAL server load, etc.
NOTE: One of these shall be present based on the data collection event		

8.2.4.7 Analytics Notification

Table 8.2.4.7-1 describes information elements for the Analytics Notification from the ADAE server to the consumer (e.g. VAL server, NF, AF).

Table 8.2.4.7-1: Analytics notification

Information element	Status	Description
Analytics ID	M	The identifier of the analytics event. This ID can be for example “VAL server performance analytics” for procedure in 8.2.2, or “VAL session performance analytics” for procedure in 8.2.3.
Analytics Output	M	The analytics outputs, which can be predictive or statistical parameter.
> VAL server performance analytics output	O (see NOTE)	Statistics or predictions of the VAL server performance, such as RTT, average/peak throughput, jitter, QoE measurements, QoS profile load, VAL server load, VAL server predicted or expected performance change for the requesting consumer.
> VAL session performance analytics output	O (see NOTE)	Statistics or predictions of the VAL session performance, such as RTT, average/peak throughput, jitter, QoE measurements, QoS profile load, VAL application traffic load, VAL session predicted or expected performance change.
Applicable area	M	The service area or geographical area for which the analytics output applies to.
Confidence level	O (see NOTE)	The achieved confidence level.
Time horizon	O (see NOTE)	The time horizon for predictive analytics.
> Start time	O	The start time point of predictive validity. If omitted, the default value is the current time.
> End time	M	The end time point of predictive validity.
NOTE: One of the IEs shall be present based on the Analyitcs ID provided in the subscription request.		

8.2.4.8 Data producer profile

The data producer profile IE includes information about the data generation/production capability of the data producer to support data collection for data analytics service and the availability/accessibility of the generated/produced data, as defined in Table 8.2.4.8-1.

Table 8.2.4.8-1: Data producer profile

Information element	Status	Description
Data Producer ID	M	ID of the data producer.
Data producer type (NOTE)	M	Specifies the type of the data producer, e.g., ADAEC, A-DCCF, A-ADRF, VAL server, SEAL server, SEAL client, EES, EAS.
Data type (NOTE)	M	Type of information that can be provided by the data producer, e.g., performance indicators, reproducer usage data, server load data, application performance, edge load.
Data producer role (NOTE)	O	Role of the data producer, e.g., generating entity, original producer, repository.
Original producer ID (NOTE)	O	If the data producer role is not “original producer” or “generating entity”, specifies the Producer ID of the original data producer for the data provided by this data producer. If the data producer type is A-DCCF, this is a list of Data Producer IDs.
Data freshness (NOTE)	O	If the data producer role is not “original producer” or “generating entity”, length of time elapsed after the data is generated until is available at the data producer. Alternatively, the data collection rate supported by the producer is provided.
Data producer capability (NOTE)	O	Indicates data producer capabilities for this data type, e.g. how long the data can be stored, support for anonymization, data generation rate and schedule.
NOTE: When the Data producer profile IE is used for Target data producer profile criteria (e.g. Table 8.2.4.4-1), this IE may be a list of values.		

8.3 Procedure on support for slice-specific application performance analytics

8.3.1 General

This clause describes the procedure for supporting slice-specific application performance analytics. The ADAES service consumer can subscribe and receive notifications about slice specific application performance analytics events. In case that the ADAES consumer needs information about historical data, the procedure in 8.7.3 can be used for retrieving of slice-specific application performance metrics data about a specific area and time window in the past.

8.3.2 Procedure

Figure 8.3.2-1 illustrates the procedure where the VAL server performance analytics are performed based on data collected from the ongoing VAL sessions as well as data from the DN (VAL server, DN database or networking stack at DN) for a specific slice.

Pre-conditions:

1. ADAEC is connected to ADAES.

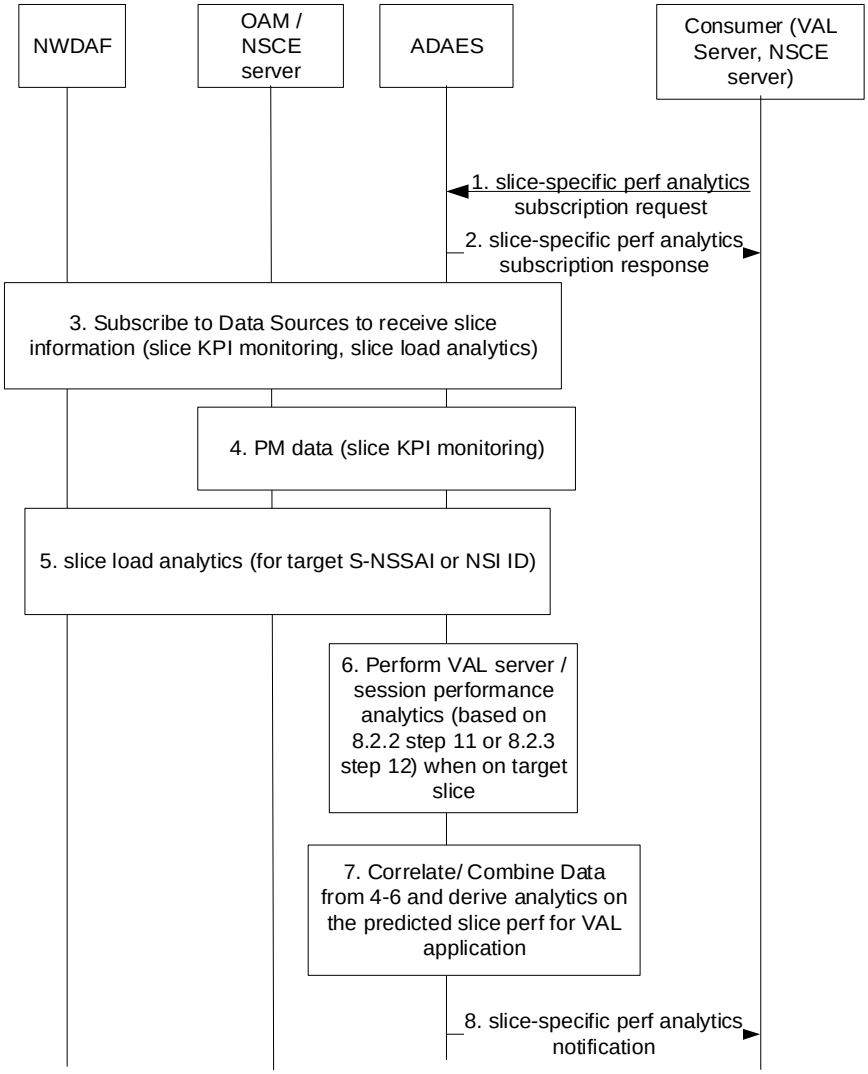

Figure 8.3.2-1: ADAES support for slice-related performance analytics

1. The consumer of the ADAES analytics service sends a subscription request to ADAES and provides the analytics event ID e.g. "slice-specific application performance analytics ", the target S-NSSAI, DNN, NSI ID, the time validity of the request, the required confidence level, area and time horizon, etc.

2. The ADAES sends a subscription response as an ACK to the consumer.

3. The ADAES subscribes to the Data Sources with the respective Data Collection Event ID and the requirement for data collection related to the request slice(s). Such requests may be towards:

   - OAM for providing PM data related to the requested slice / NSI. Alternatively, if the interaction to OAM happens via NSCE layer (see TS 23.435 [6]), such subscription can be performed to NSCE (where ADAES is acting as VAL server).

   - NWDAF for providing slice related analytics for the given area and time horizon (indicated in step 1). Such analytics can be the slice load level related network data analytics, or the service experience related network data analytics for a given slice.

4. The ADAES based on subscription, receives PM data notification from OAM or from NSCE server (via OAM APIs or NSCE-S APIs)

5. The ADAES based on subscription, receives the requested NWDAF analytics outputs. Such analytics can be:

   - network slice or NSI statistics or predictions (clause 6.3.3A of TS 23.288 [4])

   - per slice instance service experience stats or predictions (clause 6.4.3 of TS 23.288 [4])

6. The ADAES can also provide analytics on the VAL session performance (based on the procedure of clause 8.2.2 step 11 or clause 8.2.3 step 12) and filters the analytics only for the sessions which are connected to that requested slice for the area of interest.

7. The ADAES abstracts or correlates the data/analytics from steps 4-6 and provides analytics on the slice or NSI performance for the target VAL application/server. For example, such analytics can be about the min/average/max predicted RTT / end to end latency for the VAL application/server if this server uses a given slice/NSI (or for a list of given slices) within an area of interest.

8. The ADAES sends the analytics to the consumer, as a slice-specific performance analytics notification message.

8.3.3 Information flows

8.3.3.1 General

The following information flows are specified for slice-specific application performance analytics based on 8.3.2.

8.3.3.2 Slice-specific performance analytics subscription request

Table 8.3.3.2-1 describes information elements for the slice-specific performance analytics subscription request from the consumer (VAL server / NSCE server) to the ADAE server.

Table 8.3.3.2-1: Slice-specific performance analytics subscription request

Information element	Status	Description
Consumer ID	M	The identifier of the analytics consumer.
Analytics ID	O	The identifier of the analytics event. This ID can be for example “slice-specific application performance analytics”.
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions.
Slice identifier(s)	M	The identifier(s) of the target slice(s) or slice instance(s), i.e. S-NSSAI, NSI ID or ENSI.
DNN	O	The target DNN for which the request applies.
Target VAL UE ID(s)	O	The VAL UE(s) for which the analytics subscription applies.
Target VAL server ID	O	If consumer is different from the VAL server, this identifier shows the target VAL server for which the analytics subscription applies (for procedure in clause 8.3.2).
Target VAL service ID	O	The identifier of the VAL service for which the analytics applies.
Preferred confidence level	O	The required level of accuracy for the analytics service (in case of prediction).
Area of Interest	O	The geographical or service area for which the subscription request applies.
Time validity	O	The time validity of the subscription request.
Time horizon	O	The required time horizon for predictive analytics.
> Start time	O	The start time point of predictive validity. If omitted, the default value is the current time.
> End time	M	The end time point of predictive validity.
Reporting requirements	O	It describes the requirements for analytics reporting. This requirement may include e.g. the type and frequency of reporting (periodic or event triggered), the reporting periodicity in case of periodic, and reporting thresholds.

8.3.3.3 Slice-specific performance analytics subscription response

Table 8.3.3.3-1 describes information elements for the slice-specific performance analytics subscription response from the ADAE server to the consumer (VAL/NSCE server).

Table 8.3.3.3-1: Slice-specific performance analytics subscription response

Information element	Status	Description
Result	M	The result of the analytics subscription request (positive or negative acknowledgement).

8.3.3.4 Slice-specific performance analytics notification

Table 8.3.3.4-1 describes information elements for the slice-specific performance analytics notification from the ADAE server to the Consumer.

Table 8.3.3.4-1: Slice-specific performance analytics notification

Information element	Status	Description
Analytics ID	O	The identifier of the analytics event. This ID can be for example “slice-specific application performance analytics”.
Analytics Output	M	The predictive or statistical parameter on performance for the target VAL application/server, with the target slice or slice instance (e.g. the min/average/max predicted RTT / end to end latency for the VAL application/server if this server uses a given slice/NSI (or for a list of given slices) in the area of interest).
Confidence level	O (NOTE)	For predictive analytics, the achieved confidence level.
Time horizon	O (NOTE)	The time horizon for predictive analytics.
> Start time	O	The start time point of predictive validity. If omitted, the default value is the current time.
> End time	M	The end time point of predictive validity.
NOTE: These information elements shall be provided for the predictive analytics.		

8.4 Procedure on support for UE-to-UE application performance analytics

8.4.1 General

This clause describes the procedure for supporting UE-to-UE application performance analytics.

8.4.2 Procedure

Figure 8.4.2-1 illustrates the procedure where the VAL session performance analytics are performed based on data collected from the ongoing VAL UE-to-UE sessions.

Pre-conditions:

1. ADAECs are connected to ADAES.

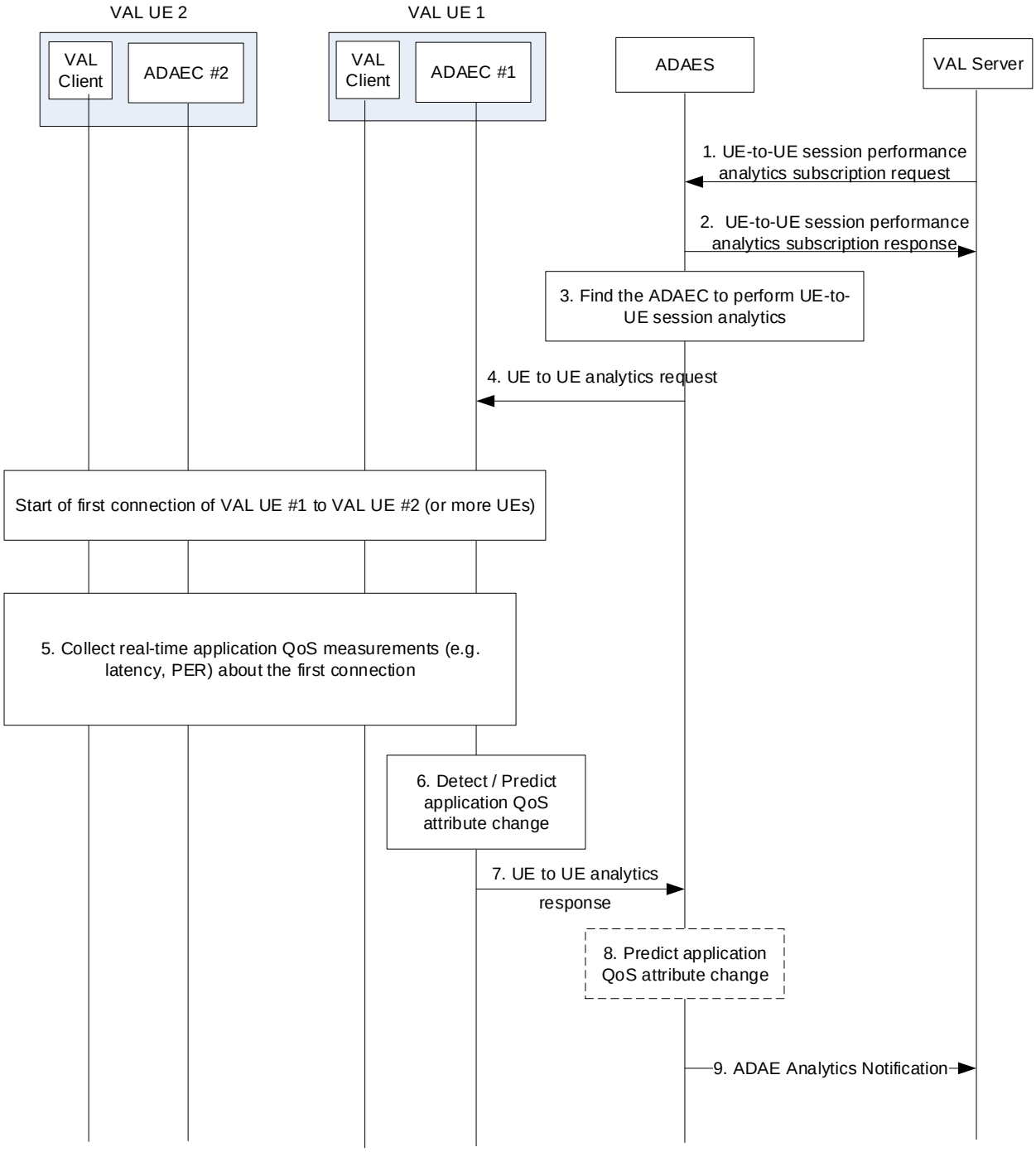

Figure 8.4.2-1: ADAES support for UE-to-UE application performance analytics

1. The consumer of the ADAES analytics service sends a subscription request to ADAES and provides the analytics event ID e.g. "UE-to-UE session performance analytics", the target VAL UE ID or group of UE IDs, the VAL service ID, the time validity and area of the request, the required confidence level, exposure level for providing UE to UE analytics. Such request can also include whether the analytics notification shall be periodic or based on an expected application QoS change (in that case also the thresholds can be provided at the request)

2. The ADAES sends a subscription response as an ACK to the consumer.

3. The ADAES selects the corresponding ADAEC #1 of the VAL UE 1 where the session performance analytics need to be performed. Such UE can be for example a capable and authorized UE from the involved VAL UE(s) within the service or group, e.g. a group lead.

4. The ADAES sends a UE-to-UE analytics request to the ADAEC #1 with the analytics ID e.g. "UE-to-UE analytics" and the configuration of the reporting required (e.g., periodic, event triggered based on threshold(s)).

Such request also includes the application QoS attributes to be analyzed (latency, bitrate, jitter, application layer PER). A session starts between the VAL UE #1 and a VAL UE #2 (or more VAL UEs).

5. The ADAEC #1 starts collecting data from the corresponding VAL UE(s) based on the request. Such data can be about the latency, throughput, jitter, QoE measurements, PQI load, etc. The data can be collected by ADAEC #1 from other ADAECs via ADAE-C interface, or from the VAL clients (VAL client to VAL client interaction is out of scope).

6. The ADAEC either detects or predicts an application QoS change (depending on the authorization of ADAEC to perform analytics). Such change can be for example an application QoS downgrade related to the UE-to-UE session latency, or the application layer PER/channel losses higher than a predefined threshold, for a given time horizon with a certain confidence level.

7. The ADAEC sends the analytics to the ADAES in a UE-to-UE analytics response message.

8. The ADAES based on the received response, confirms/verifies the analytics received or provides analytics (in case that data were reported) for the UE-to-UE session. Such analytics can be about predicting the application QoS change for the UE-to-UE session.

9. The ADAES sends the derived analytics notification to the consumer.

NOTE: The mechanism for analytics collection from the UE side (steps 4, 7) shall align with the SA4 mechanism for generic data collection from the UE (TS 26.531 [3]).

8.4.3 Information flows

8.4.3.1 General

The following information flows are specified for UE-to-UE session performance analytics based on 8.4.2

8.4.3.2 UE-to-UE session performance analytics subscription request

Table 8.4.3.2-1 describes information elements for the UE-to-UE session performance analytics subscription request from the consumer (VAL server) to the ADAE server.

Table 8.4.3.2-1: UE-to-UE session performance analytics subscription request

Information element	Status	Description
VAL server ID	M	The identifier of the analytics consumer (VAL server).
Analytics ID	O	The identifier of the analytics event. This ID can be equivalent to “UE-to-UE session performance analytics”.
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions.
Analyitcs category	M	The category of analytics for the event, e.g. performance change, performance sustainability for given QoS parameters (e.g., latency, PER, bitrate, jitter), or both.
VAL UE ID(s) and address(es)	M	The VAL UE identifier(s) and IP address(es) for which the analytics subscription applies.
VAL service ID	O	The identifier of the VAL service for which the subscription applies.
Preferred confidence level	O	The required level of accuracy for the analytics service (in case of prediction).
Area of Interest	O	The geographical or service area for which the subscription request applies.
Time validity	O	The time validity of the subscription request.
Exposure level requirement	O	The level of exposure requirement (e.g. condition on providing the analytics like threshold is reached) for the analytics to be exposed.
Reporting requirements	O	It describes the requirements for analytics reporting. This requirement may include e.g. the type and frequency of reporting (periodic or event triggered (e.g. based on an expected application QoS change) with the reporting granularity (e.g. individual session or group of sessions), the reporting periodicity in case of periodic, and reporting thresholds in case of event triggered.

8.4.3.3 UE-to-UE session performance analytics subscription response

Table 8.4.3.3-1 describes information elements for the UE-to-UE session performance analytics subscription response from the ADAE server to the VAL server.

Table 8.4.3.3-1: UE-to-UE session performance analytics subscription response

Information element	Status	Description
Result	M	The result of the analytics subscription request (positive or negative acknowledgement).

8.4.3.4 UE-to-UE analytics request

Table 8.4.3.4-1 describes information elements for the UE-to-UE analytics request from the ADAE server to the ADAE client.

Table 8.4.3.4-1: UE-to-UE analytics request

Information element	Status	Description
ADAE server ID	M	The identifier of the ADAE server.
Analytics ID	O	The identifier of the analytics event (Analytics ID= UE-to-UE analytics').
VAL UE ID(s) and address(es)	M	The VAL UE identifier(s) and IP address(es) for which the data/analytics apply.
Application QoS attributes	M	The QoS attributes (latency, bitrate, jitter, application layer PER) to be analyzed at the ADAE client.
Reporting configuration	O	The configuration for analytics reporting. This requirement may include e.g. the frequency of reporting (periodic or event triggered), the reporting periodicity in case of periodic, and reporting thresholds in case of event triggered, whether data abstraction is needed or not.
Data collection requirements	O	The requirements for data collection, including the format of data, frequency of reporting, level of abstraction of data, level of accuracy of data.
Area of Interest	O	The geographical or service area for which the request applies.
Time validity	O	The time validity of the request.

8.4.3.5 UE-to-UE analytics response

Table 8.4.3.5-1 describes information elements for the UE-to-UE analytics response from the ADAE client to the ADAE server.

Table 8.4.3.5-1: UE-to-UE analytics response

Information element	Status	Description
Analytics ID	M	The identifier of the analytics event.
VAL UE ID(s) and address(es)	M	The VAL UE identifier(s) and IP address(es) for which the analytics apply.
Analytics Output	M	The reported analytics for the UE to UE sessions, which can be in form of offline stats/historical data or predictions on the requested QoS parameter based on the analytics event.

8.4.3.6 ADAE Analytics Notification

Table 8.4.3.6-1 describes information elements for the ADAE Analytics Notification from the ADAE server to the consumer (VAL server).

Table 8.4.3.6-1: ADAE Analytics notification

Information element	Status	Description
Analytics ID	O	The identifier of the analytics event. This ID can be "UE-to-UE session performance analytics".
Analytics Output	M	The analytics outputs, which can be predictive or statistical parameter.
> Performance change	O (NOTE)	A VAL UE to UE session predicted or expected performance change.
>> Time for change	M	The predicted or expected time when the performance change happens.
>> Confidence level	O	The achieved confidence level for the predictive analytics.
> Performance sustainability	O (NOTE)	A VAL UE to UE session performance sustainability over a given time horizon/area.
>> Time horizon	M	The time horizon for predictive analytics.
>>> Start time	O	The start time point of predictive validity. If omitted, the default value is the current time.
>>> End time	M	The end time point of predictive validity.
>> Applicable area	M	The service area or geographical area for which the analytics output applies to.
>> Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
NOTE: At least one of the IEs shall be present based on the Analytics category IE provided in the subscription request.		

8.5 Procedure on support for location accuracy analytics

8.5.1 General

This clause describes the procedure for supporting location accuracy analytics.

8.5.2 Procedure

Figure 8.5.2-1 illustrates the procedure for location accuracy analytics enablement solution.

Pre-conditions:

1. ADAES is connected to A-ADRF.
2. ADAES has discovered SEAL LMS or FLS.

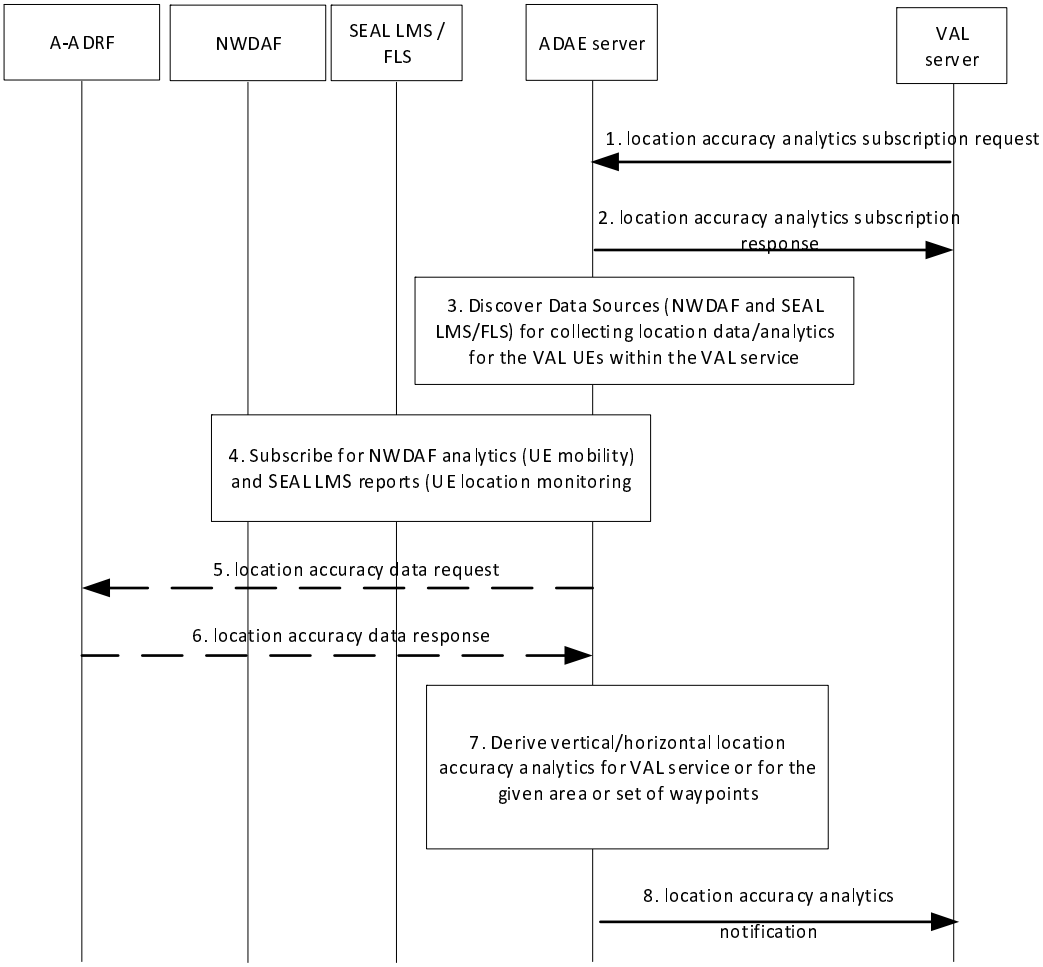

Figure 8.5.2-1: Location accuracy analytics procedure

1. The VAL server makes a subscription request to ADAE server for location accuracy prediction/stats, including an analytics event ID (e.g. "location accuracy prediction" or "location accuracy sustainability"), an analytics request type (if not identified specifically at the event ID) which can be the location accuracy prediction for a given location X and/or for a given UE/app. The request may include also the target area, a target VAL service, or a VAL UE, or group of UEs of the VAL service, time validity, accuracy threshold and requirements. If the VAL UEs are provided by the VAL server, this request may also include the expected route or a set of waypoints for the UEs of the VAL application.

2. The ADAE server sends a location accuracy analytics subscription response as an ACK to the VAL server.

3. The ADAE server discovers and maps the Data Sources with the respective analytics event ID for collecting location data for the corresponding VAL UEs or VAL service area.

4. The ADAE server subscribes for NWDAF UE mobility analytics per VAL UE (for all the VAL UEs) and gets notification on the per UE location/mobility analytics based on TS 23.288 clause 6.7.2. Such analytics may be requested for a list of waypoints per UE route (if indicated at step 1). The ADAE server subscribes also for SEAL LMS location reports for the respective VAL UEs or location reports from all VAL UEs within the requested area.

5. The ADAE server optionally requests location accuracy historical analytics /data from A-ADRF for the corresponding VAL UEs or VAL service area.

6. Based on the request, the ADAE server receives location accuracy historical analytics /data from A-ADRF for the corresponding VAL UEs or VAL service area.

7. The ADAE server abstracts or correlates the data/analytics from steps 4-6 and provides analytics on the location accuracy for the target VAL application. Depending on the event ID in step 1, the ADAE server can indicate whether the location accuracy is sustainable or is predicted to be downgraded or can be upgraded and become more granular (e.g. from meter to decimetre).

8. The ADAE server sends the location accuracy analytics notification to the consumer.

8.5.3 Information flows

8.5.3.1 General

The following information flows are specified for location accuracy analytics based on 8.5.2

8.5.3.2 Location accuracy analytics subscription request

Table 8.5.3.2-1 describes information elements for the location accuracy analytics subscription request from the VAL server to the ADAE server.

Table 8.5.3.2-1: Location accuracy analytics subscription request

Information element	Status	Description
VAL server ID	M	The identifier of the VAL server.
Analytics ID	M	The identifier of the location accuracy analytics event. This ID can be for example "location accuracy prediction" or "location accuracy sustainability" depending on the expected outcome.
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions.
VAL UE ID(s) or Group ID	M	The identity of the VAL UE(s) or group of UEs for which the analytics subscription applies
VAL service ID	O	The identifier of the VAL service for which location accuracy analytics is requested.
Location accuracy requirements	M	The accuracy threshold and VAL requirements.
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction).
Area of Interest	O	The geographical or service area for which the subscription request applies.
Time validity	O	The time validity of the subscription request.
UE mobility / route information	O	Information on the target UE or group UE mobility including the expected route/set of waypoints.
Reporting requirements	O	It describes the requirements for analytics reporting. This requirement may include e.g. the type and frequency of reporting (periodic or event triggered), the reporting periodicity in case of periodic, and reporting thresholds.

8.5.3.3 Location accuracy analytics subscription response

Table 8.5.3.3-1 describes information elements for the location accuracy analytics subscription response from the ADAE server to the VAL server.

Table 8.5.3.3-1: Location accuracy analytics subscription response

Information element	Status	Description
Result	M	The result of the analytics subscription request (positive or negative acknowledgement)

8.5.3.4 Location accuracy data request

Table 8.5.3.4-1 describes information elements for the location accuracy data request from the ADAE server to the A-ADRF.

Table 8.5.3.4-1: Location accuracy data request

Information element	Status	Description
ADAE server ID	M	The identifier of the ADAE server
Analytics ID	M	The identifier of the analytics event
List of VAL UE IDs and addresses	M	The VAL UE(s) identifiers and IP address(es) for which the data/analytics apply
VAL service ID	O	The service ID, in case of requesting historical data for a particular VAL service.
Reporting configuration	O	The configuration for data reporting. This requirement may include e.g. the frequency of reporting (periodic), the reporting periodicity in case of periodic, and reporting thresholds, whether data abstraction is needed or not.
Data collection requirements	O	The requirements for data collection, including the format of data, frequency of reporting, level of abstraction of data, level of accuracy of data.
Area of Interest	O	The geographical or service area for which the subscription request applies
Time validity	O	The time validity of the request

8.5.3.5 Location accuracy data response

Table 8.5.3.5-1 describes information elements for the location accuracy data response from the A-ADRF to the ADAE server.

Table 8.5.3.5-1: Location accuracy data response

Information element	Status	Description
Analytics ID	M	The identifier of the analytics event.
List of VAL UE IDs and addresses	M	The VAL UE(s) identifiers and IP address(es) for which the analytics apply
VAL service ID	O	The service ID, in case of requesting historical data for a particular VAL service.
Analytics Output	M	The reported analytics for the location accuracy, which can be in form of offline stats/historical data for a specific VAL service or for particular UE(s) or group of UEs

8.5.3.6 Location accuracy analytics notification

Table 8.5.3.6-1 describes information elements for the location accuracy analytics notification from the ADAE server to the VAL server.

Table 8.5.3.6-1: Location accuracy analytics notification

Information element	Status	Description
Analytics ID	M	The identifier of the analytics event.
VAL UE ID(s)	O	The identity of the VAL UE(s) for which the analytics applies.
VAL service ID	O	The identifier of the VAL service for which location accuracy analytics applies.
Analytics Output	M	The analytics outputs, which can be predictive or statistical parameter
> Location accuracy prediction	O (see NOTE)	A predicted or expected location accuracy change (downgrade or upgrade) for a particular VAL service or UEs. The IE shall be provided if the Analytics ID is "location accuracy prediction".
>> Applicable area	O	A list of service area or geographical area for which the analytics applies to.
>> Applicable time period	O	The time period that the analytics applies to.
>> Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
> Location accuracy sustainability	O (see NOTE)	The location accuracy sustainability for a VAL service or UE/group of UEs over a given time horizon/area. The IE shall be provided if the Analytics ID is "location accuracy sustainability".
>> Applicable area	O	A list of service area or geographical area for which the analytics applies to.
>> Applicable time period	O	The time period that the analytics applies to.
>> Crossed reporting threshold(s)	O	The Reporting Threshold(s) that are met or exceeded or crossed by the statistics value or the expected value of the location accuracy.
>> Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
NOTE: At least one of the IEs shall be present.		

8.6 Procedure for supporting service API analytics

8.6.1 General

This clause describes the procedure for supporting service API analytics. Such analytics can be for one or more service APIs for a service produced by one or more service producers within the 5GS or enablement layer or the DN side (e.g., application server).

8.6.2 Procedure

Figure 8.6.2-1 illustrates the procedure for service API analytics enablement solution.

Pre-conditions:

1. ADAES acts as API management function in CAPIF

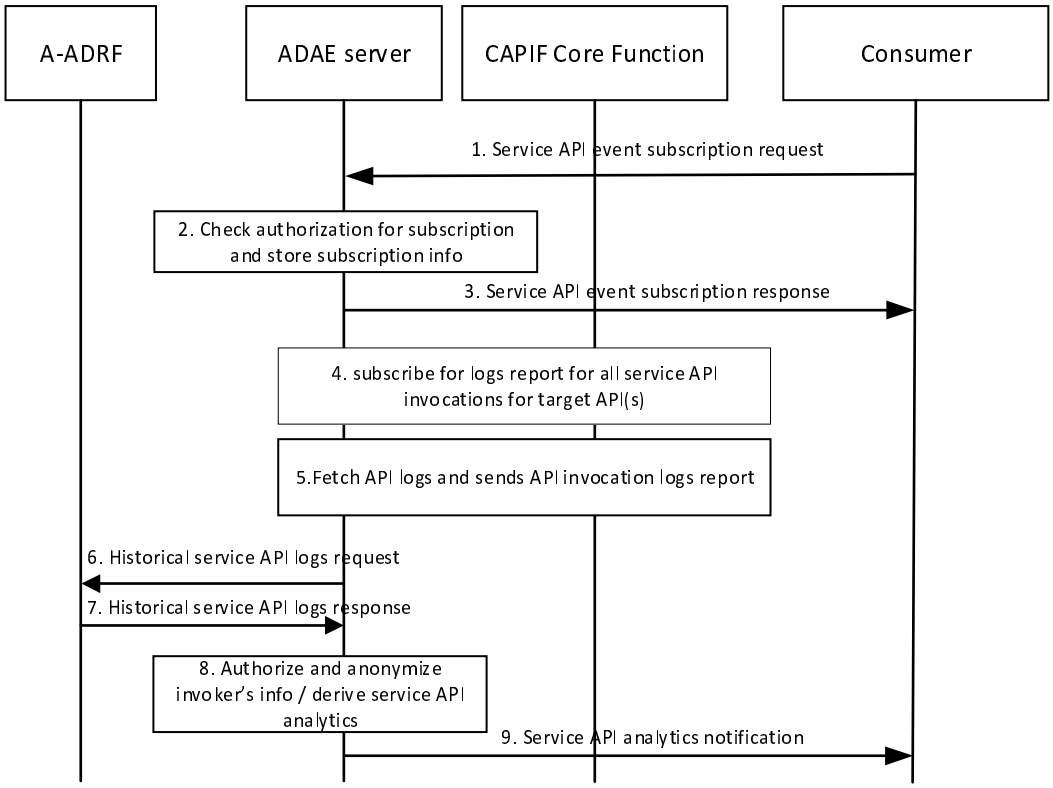

Figure 8.6.2-1: Service API analytics procedure

1. The consumer (VAL server, API provider) sends a service API event subscription request to the ADAE server to receive analytics for one or more service APIs.

2. Upon receiving the subscription request from the subscribing entity, the ADAE server checks for the relevant authorization for the event subscription. If the authorization is successful, the ADAE server stores the subscription information.

3. The ADAE server sends a service API event subscription response indicating successful subscription.

4. Upon sending the subscription response, the ADAE server requests to collect API logs to be used to derive analytics and triggers API invocation log pull request towards the CAPIF core function. The API invocation log fetch request indicates the API (or list of APIs) for which logs are required. Based on the ADAE server deployment, this can be a Query service API log request which is performed via CAPIF_Auditing API as specified in 3GPP TS 23.222 [8].

5. The CCF authorizes the request and fetches the API logs from the storage unit. CCF then sends the requested information to the ADAE server via a query service API log response.

6. The ADAES may also request service API historical analytics /data from A-ADRF for the corresponding service APIs.

7. Based on the request, the ADAES receives historical analytics/data for the service APIs from the A-ADRF.

8. The ADAE server authorizes and anonymizes the API logs (if not performed by CCF) and abstracts based on exposure level. The exposure level can be known based on pre-configuration by the OAM or based on the subscription and type of invoker. The ADAE server then derives analytics on the target service API(s) based on the logs received from the CCF. Such analytics are predictions/stats for the API status based on the analytics event.

9. The ADAE server sends the analytics as event notifications to all the subscribing entities that have subscribed for the event matching the criteria. If a notification reception information is available as part of the subscribing entity event subscription, then the notification reception information is used by the ADAE server to send event notifications to the subscribing entity.

8.6.3 Information flows

8.6.3.1 General

The following information flows are specified for service API analytics based on 8.6.2.

8.6.3.2 Service API event subscription request

Table 8.6.3.2-1 describes information elements for the service API event subscription request from the consumer (VAL server, API provider) to the ADAE server.

Table 8.6.3.2-1: Service API event subscription request

Information element	Status	Description
Consumer ID	M	The information to determine the identity of the subscribing entity (consumer).
Service API information	M	The service API name or type.
Analytics ID	O	The identifier of the analytics event. This ID can be for example “service API analytics”.
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions.
Criteria	M	The event criteria include event type information relevant to the prediction or stats on the number of failure API invocations, API availability, frequency and occurrence of API version changes, API location changes for the target API, etc.
Time Validity	O	Time validity of the subscription request.
Time horizon	O	The time horizon for predictive analytics.
> Start time	O	The start time point of predictive validity. If omitted, the default value is the current time.
> End time	M	The end time point of predictive validity.
Area of interest	O	Geographical or topological area for which the subscription applies.
Notification reception information	O	The information of the subscribing entity for receiving the notifications for the event.
Reporting requirements	O	It describes the requirements for analytics reporting. This requirement may include e.g. the type and frequency of reporting (periodic or event triggered), the reporting periodicity in case of periodic, and reporting thresholds in case of event triggered.

8.6.3.3 Service API event subscription response

Table 8.6.3.3-1 describes information elements for the service API event subscription response to the consumer (VAL server, API provider) from the ADAE server.

Table 8.6.3.3-1: Service API event subscription response

Information element	Status	Description
Result	M	The result of the analytics subscription request (positive or negative acknowledgement).

8.6.3.4 Historical service API logs request

Table 8.6.3.4-1 describes information elements for the historical service API logs request from the ADAE server to the A-ADRF.

Table 8.6.3.4-1: Historical service API logs request

Information element	Status	Description
Service API log requestor information	M	Identity information of the originated application querying service API log request.
ADAES ID	M	Identity information of the ADAES.
Service ID or UE ID	M	Identity of the application service or UE for which the historical API invocations apply.
Target API(s) information	M	Information on target API or list of target APIs (name or type).
>Query information	O	List of query filters such as invoker's ID and IP address, service API name and version, input parameters, and invocation result.
> API aggregation abstraction flag	O	What type of aggregation or abstraction/filtering needs to be applied.
Reporting configuration	O	The configuration for the logs reporting. This requirement may include e.g. reporting thresholds, whether data abstraction is needed or not.
Area of validity	O	The geographical area for which the request applies.
Time validity	O	The time validity for the request.
Exposure level requirement	O	The level of exposure requirement (e.g. permissions on the logs like read/write/delete) for the logs to be exposed.

8.6.3.5 Historical service API logs response

Table 8.6.3.5-1 describes information elements for the historical service API logs response to the ADAE server from the A-ADRF.

Table 8.6.3.5-1: Historical service API logs response

Information element	Status	Description
Result	M	Identity information of the originated application querying service API log request.
VAL service ID or UE ID	M	Identity of the application service or UE for which the API invocations apply.
Target API (s) information	M	The target service API name or type.
>Target API(s) logs	M	The API logs based on the subscription event. This may include the number of failure API invocations, API availability, frequency and occurrence of API version changes, API location changes for the target API, API throttling events, number of API invocations for a given area and time etc.
>Reporting info	O	The time and area for which the reporting applies.

8.6.3.6 Service API analytics notification

Table 8.6.3.6-1 describes information elements for the service API analytics notification to the subscriber/consumer from the ADAE server.

Table 8.6.3.6-1: Service API analytics notification

Information element	Status	Description
Service API information	M	The service API name or type for which analytics apply.
Analytics ID	O	The identifier of the analytics event. This ID can be for example “service API analytics”.
Analytics Output	M	Stats or predictions based on abstracted or anonymized API logs (for example number of failure API invocations, API availability, frequency and occurrence of API version changes, API location changes for the target API, API throttling events, number of API invocations for a given area and time, API load statistics for a given edge network, etc).
Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
Area of validity	O	Geographical or topological area for which the analytics apply.

8.7 Slice usage pattern analytics

8.7.1 General

This clause provides a procedure for network slice usage pattern analytics based on collected network slice performance and analytics, historical network slice status, and network performance. The analytics consumer can be either the VAL server or other analytics consumers such as SEAL NSCE server.

8.7.2 Procedure on slice usage pattern analytics

Figure 8.7.2-1 illustrates the procedure for network slice usage pattern analytics.

Pre-conditions:

1. The ADAES is registered and capable of interacting with 5GS to collected network slice data.

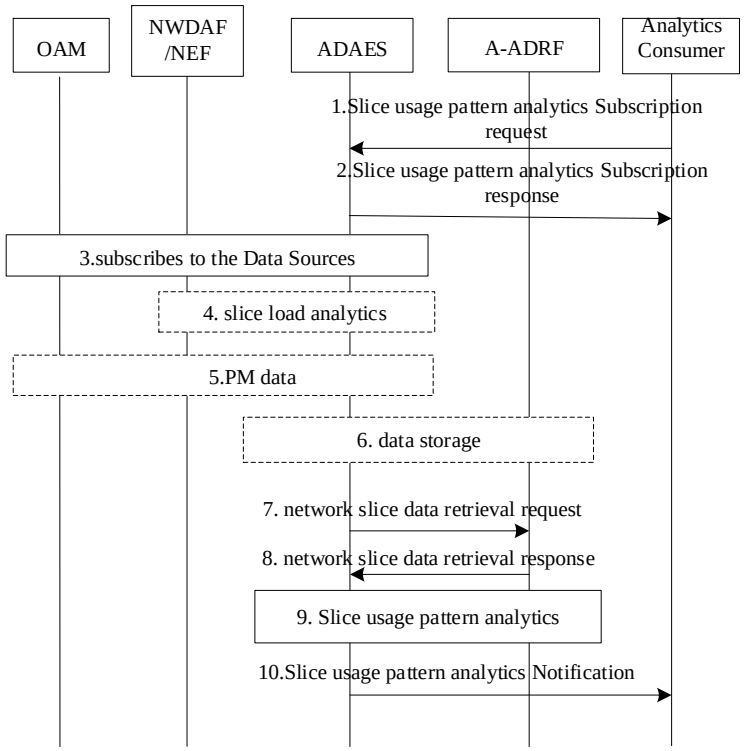

Figure 8.7.2-1: Procedure for network slice usage pattern analytics

1. The analytics consumer (VAL server/NSCE server) sends a slice usage pattern analytics subscription request to ADAES and provides the target S-NSSAI, DNN, area of the interest, interest time period of the historical data (e.g., last year), the required confidence level, etc. Optionally, the slice requirement could also be provided.

2. The ADAES sends a slice usage pattern analytics subscription response to the analytics consumer.

3. The ADAES subscribes to the Data Sources with the respective Data Collection Event ID and the requirement for data collection related to the request slice(s). Such requests can be sent to OAM, NWDAF or the combination of them.

4. Based on subscription, the ADAES may receive Network slice related Observed Service experience statistics, Load level information of a Network Slice from NWDAF (or via NEF) as defined in TS 23.288 [4].

5. Based on subscription, the ADAES may receive Network slice / NSI related performance data from OAM as defined in TS 28.552 [7] and the alarms of network slice instances from OAM system via the procedures defined in clause 6.1 of TS 28.545 [12].

6. If the data is collected from multiple sources, the ADAES combines or correlates the data/analytics from steps 3-5 and stores the data into A-ADRF if needed.

7. The ADAES server sends the network slice data retrieval request to collect the historical data from A-ADRF.

8. The A-ADRF provides network slice historical data to the ADAES.

9. The ADAES analyzes the network slice usage pattern based on the network slice historical data and collected slice performance. When the stored historical data does not cover the required interest time period of the historical data, ADAES analyzes the slice usage pattern based on the existing stored historical data.

10. The ADAES sends the slice usage pattern analytics notification to the analytics consumer.

8.7.3 Procedure on retrieving slice usage statistics data

In the procedure shown in Figure 8.7.3-1, a mechanism is provided to allow for vertical/ASP using VAL server, NSCE server to initiate request for retrieving of statistics data and receive all the historical data for a specific time window.

Pre-conditions:

1. Enterprise hosting the VAL server or NSCE server has SLA for analytics services with ADAES service provider.
2. The VAL server or NSCE server has subscribed to slice usage patterns analytics from ADAES, and statistics are available.
3. The VAL server or NSCE server has identified there is specific statistics data needed in a specific time window.

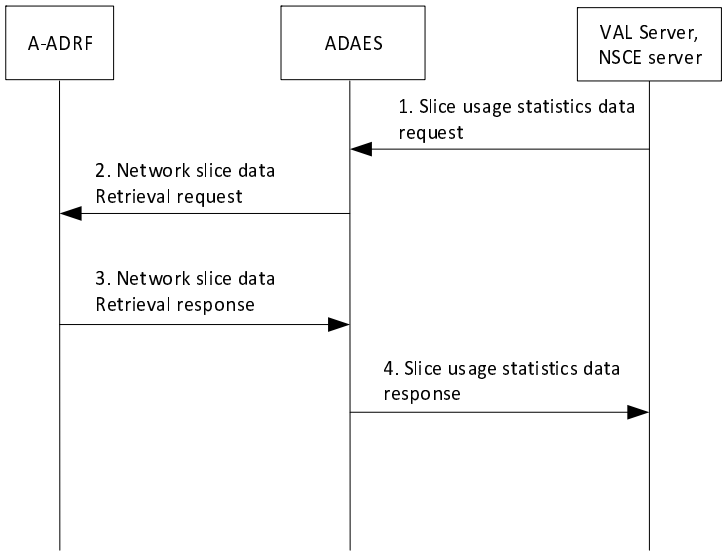

Figure 8.7.3-1: Retrieving of slice usage statistics data procedure

1. The VAL server/NSCE server sends to ADAES server a slice usage statistics data request containing information about specific time and needed statistics parameters.
2. ADAES server, based on the input in step 1, determines the needed analytics ID and data producer IDs, slice metrics for a specific slice area and specific period of time and uses the network slice data retrieval request to request the needed data from the A-ADRF.
3. A-ADRF sends back the network slice data retrieval response with the required information from its database.
4. The ADAES sends slice usage statistics data response to VAL server/NSCE server.

8.7.4 Information flows

8.7.4.1 General

The following information flows are specified for network slice usage pattern analytics based on 8.7.2.

8.7.4.2 Network slice usage pattern analytics subscription request

Table 8.7.4.2-1 describes information elements for the network slice usage pattern analytics subscription request from the analytics consumer (VAL server / NSCE server) to the ADAE server.

Table 8.7.4.2-1: Network slice usage pattern analytics subscription request

Information element	Status	Description
Consumer ID	M	The identifier of the analytics consumer
Analytics ID	O	The identifier of the analytics event. This ID can be for example “Network slice usage pattern analytics”.
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions.
Analytics filter information	M	Filter information for the analytics event.
>Slice identifier	M	The identifier of the target slice or slice instance, i.e. S-NSSAI.
>Slice requirement	O	The requirement of network requirements or updated requirements when the network slice was created. The GST defined by GSMA (see clause 2.2 in [10]) and the performance requirements defined in clause 7 of TS 22.261 [11] are all considered as input for the network slice related requirements.
>DNN	O	The target DNN for which the request applies.
>Target VAL UE ID(s)	O	The VAL UE(s) for which the analytics subscription applies
>Target VAL server ID	O	If consumer is different from the VAL server, this identifier shows the target VAL server for which the analytics subscription applies.
>Area of Interest	O	The geographical or service area for which the subscription request applies.
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction.
Time validity	O	The time validity of the request.
Interest time period of the historical data	O	Interest time period of the historical data (e.g. last year),
Reporting requirements	O	It describes the requirements for analytics reporting. This requirement may include e.g. the type and frequency of reporting (periodic or event triggered), the reporting periodicity in case of periodic, and reporting thresholds in case of event triggered.

8.7.4.3 Network slice usage pattern analytics subscription response

Table 8.7.4.3-1 describes information elements for the Network slice usage pattern analytics subscription response from the ADAE server to the analytics consumer (VAL/NSCE server).

Table 8.7.4.3-1: Network slice usage pattern analytics subscription response

Information element	Status	Description
Successful response (NOTE)	O	Indicates that the request was successful.
Failure response (NOTE)	O	Indicates that the request failed.
> Cause	O	Indicates the cause of request failure.
NOTE: One of these IEs shall be present in the message.		

8.7.4.4 Network slice usage pattern analytics notification

Table 8.7.4.4-1 describes information elements for the network slice usage pattern analytics notification from the ADAE server to the analytics Consumer.

Table 8.7.4.4-1: Network slice usage pattern analytics notification

Information element	Status	Description
Analytics ID	O	The identifier of the analytics event. This ID can be for example “Network slice usage pattern analytics”.
Analytics Output	M	The predictive or statistical parameter, which can be analytics of network slice usage pattern (e.g. periodicity of slice usage peak).
Confidence level	O	For predictive analytics, the achieved confidence level can be provided.

8.7.4.5 Network slice data retrieval request

Table 8.7.4.5-1 describes information elements for the Network slice data retrieval request from the ADAE server to the A-ADRF.

Table 8.7.4.5-1: Network slice data retrieval request

Information element	Status	Description
ADAE server ID	M	The identifier of the ADAE server.
Data Collection Event ID	M	The identifier of the data collection event.
Network slice identifier	M	The identifier of the interested network slice.
VAL service ID	O	The identifier of the VAL service which is associated with network slice.
Data Collection requirements	M	The requirements for data collection, including the format of data, frequency of reporting, level of abstraction of data, level of accuracy of data.
Analytics ID	O	The identifier of the analytics event, for which the data collection is needed.
List of Data Producer IDs	O	In case when this request is performed via A-DCCF, then the list of Data Producer IDs is needed.
Target VAL UE ID(s) and address(es)	O	The VAL UE(s) identifiers and IP address(es) for which the data collection subscription apply.
Target VAL server ID	O	This identifier of the target VAL server for which the data collection subscription applies.
Area of Interest	O	The geographical or service area for which the requirement request applies.
Interest time period of the historical data	O	Interest time period of the historical data.
Time validity	O	The time validity of the request.

8.7.4.6 Network slice data retrieval response

Table 8.7.4.6-1 describes information elements for the Network slice data retrieval response from the A-ADRF to the ADAE server.

Table 8.7.4.6-1: Network slice data retrieval response

Information element	Status	Description
Data Collection Event ID	M	The result of the data collection subscription request (positive or negative acknowledgement).
Network slice identifier	M	The identifier of the interested network slice
Target VAL UE ID(s) and address(es)	O (NOTE)	The VAL UE(s) identifiers and IP address(es) for which the data apply.
Target VAL server ID	O (NOTE)	This identifier of the target VAL server for which the data applies.
Analytics ID	O	The identifier of the analytics event.
Data Type	O	The type of reported data samples which can be UE data, network data, application data, edge data, or different granularities / abstraction of data (e.g. real time, non real time).
Data Output	M	The reported data, which can be inform of measurements or offline/historical data on the requested parameter (e.g. RTT deviation) based on subscription.
Timestamp	O	Time stamp of the collected report data.
NOTE: One of these shall be present based on the data collection event.		

8.7.4.7 Slice usage statistics data request

Table 8.7.4.7-1 describe information elements for the slice usage statistics data request between the VAL server, NSCE server and the ADAE server.

Table 8.7.4.7-1: Slice usage statistics data request

Information element	Status	Description
Consumer ID	M	The identifier of the statistics consumer.
Slice usage statistics data ID	M	Identifier of the slice usage data statistics, for which the data collection is needed.
Statistics data filter information	M	Filter information for the statistics data event.
> VAL service ID	M	Identifier of the VAL service for which the request applies.
> Network slice Identifier(s)	M	Identifier(s) of the network slice for which the request applies.
> Network slice related parameters	O	Slice parameters statistics needed.
>DNN	O	The target DNN for which the request applies.
> UE(s) related Identifier(s)	O	Identifier(s) of the related UE(s).
Area of Interest	O	The geographical or service area for which the request applies.
StartTime	M	The start time point of the requested statistics data.
EndTime	M	The end time point of the requested statistics data.

8.7.4.8 Slice usage statistics data response

Table 8.7.4.8-1- describe information elements for the slice usage statistics data response between the VAL server, NSCE server and the ADAE server.

Table 8.7.4.8-1: Slice usage statistics data response

Information element	Status	Description
Result	M	Indicates the success or failure of slice usage pattern statistics data request.
Slice usage statistics data ID	M	Identifier of the slice usage data statistics.
Network slice identifier	M	The identifier of the interested network slice.
>Data output	O (NOTE 1)	The reported data related to the network slice usage pattern statistics data request.
>> Timestamp	O	Time stamp of the collected report data.
>Cause	O (NOTE 2)	Indicates the cause of the slice usage pattern statistics data request failure.
NOTE 1: Shall be present if the result is success. NOTE 2: Shall be present if the result is failure.		

8.8 Procedure for supporting edge load analytics

8.8.1 General

This clause describes two procedures (covering both subscribe-notify and request-response models in 8.8.2.1 and 8.8.2.2 respectively) for supporting edge load analytics, where the edge analytics are performed based on data collected from the EDN (EAS and/or EES) and A-ADRF.

8.8.2 Procedure

8.8.2.1 Subscribe-notify model

Figure 8.8.2.1-1 illustrates the procedure for edge load analytics enablement solution.

Pre-conditions:

1. ADAES has discovered the APIs to access the edge services at EDN.
2. ADAES has subscribed to OAM and NWDAF for receiving management and DN performance analytics respectively.
3. Data producers (e.g. A-ADRF, EAS, EES) may be pre-configured with data producer profiles (as in Table 8.2.4.8-1) for the data they can provide. ADAES and ADAEC have discovered available data producers and their data producer profiles.

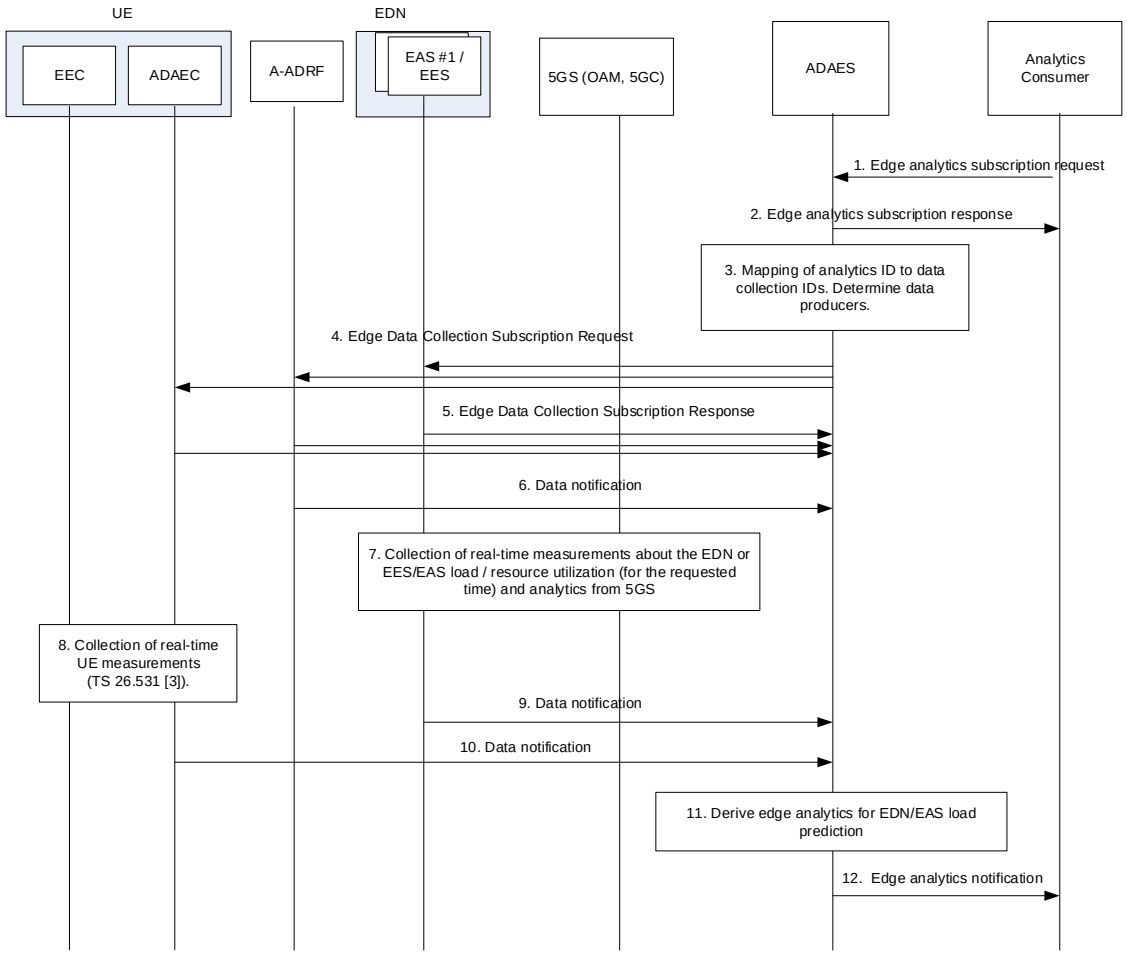

Figure 8.8.2.1-1: ADAES support for edge analytics

1. The consumer of the ADAES analytics service sends an edge analytics subscription request to ADAES.
2. The ADAES sends an edge analytics subscription response as an ACK to the analytics consumer.
3. The ADAES maps the analytics event ID to a list of data collection event identifiers, and a list of data producer IDs. Such mapping may be preconfigured by OAM or may be determined by ADAES based on the analytics event ID and/or data producer profile (Table 8.2.4.8-1). Such Data Producers can be EASs onboarded to EDN, EESs, A-ADRF, as well as MEC Platform services.
4. The ADAES sends a subscription request to the Data Producers (EASs onboarded to EDN, EESs, A-ADRF, ADAEC) or the A-DCCF with the respective Data Collection Event ID and the requirement for data collection.
5. The Data Producers (e.g., EASs onboarded to EDN, EESs, A-ADRF, ADAEC) or the A-DCCF send a subscription response as a positive or negative acknowledgement to the ADAES.
6. The ADAES based on subscription receive offline stats/data on the edge DN load based on the analytics/data collection event ID from A-ADRF. Such stats can be about the load in terms of number of EAS or EES connections for a given area or time window, or the average edge computational resource usage or usage ratio based on the EDN total resource availability, EDN overload/high load indication events, probability of EAS/EES unavailability due to high load, etc.
7. The Data Producers at the edge start collecting data from the data generating entities. Such data can be measurements or analytics based on the data source/producer, as follows:
   - from OAM or EAS/ASP (for EAS load info): Per EAS/EES computational resource load, number of connections per EES/EAS

- from N6 endpoint: N6 load
- from 5GC / NWDAF: DN performance analytics
- from OAM / MDAS: UPF load analytics (per DNAI)
- from MEC platform services (e.g., RNIS): per cell radio conditions / load for all cells within EDN coverage

NOTE 1: How the ADAES obtains the EAS load information from EAS/ASP is up to implementation.

NOTE 2: Steps 6 and 7 are not necessarily sequential and can be performed in parallel or in different order.

8. If in step 4 ADAES sent a subscription request to ADAEC as Data Producer, data collection is initiated by ADAEC from UE data generating entities.

NOTE 3: Data collection at the UE reuses the SA4 mechanism based on EVEX study (TS 26.531 [3]).

9. The edge Data Producers (targets of the subscription requests in step 4) send the data to the ADAES (based on step 7 measurements or analytics) as a data notification message. Such data can be about the load in terms of number of EAS or EES connections for a given area or time window, or the average edge computational resource usage or usage ratio based on the EDN total resource availability, EDN overload/high load indication events, probability of EAS/EES unavailability due to high load, etc.

10. ADAEC sends data (periodically or if a threshold is reached based on configuration) about the edge load as collected at the UE, e.g. in terms of number of AC or EEC connections for a given UE in a given time window, number of edge service sessions, etc.

11. The ADAES derives edge analytics on EDN / DNAI load or per EES/EAS load, based on the analytics ID and type of request. The analytics are derived based on the performance analytics received per DN or load analytics per DNAI/UPF; as well as considering measurements on the computational or RAN resource load or number of connections for the EES/EASs which are active at the EDN.

12. The ADAES sends the edge analytics to the consumer, based on the request and the derived analytics in step 9. Such analytics indicate a prediction of the EDN load considering inputs from both 5GS as well as from edge platform services. Such prediction can also be in form of a recommendation for triggering an EAS relocation to a different platform.

8.8.2.2 Request-response model

Figure 8.8.2.2-1 illustrates the procedure for the analytics consumer to request analytics data of the application server(s) from the ADAE server.

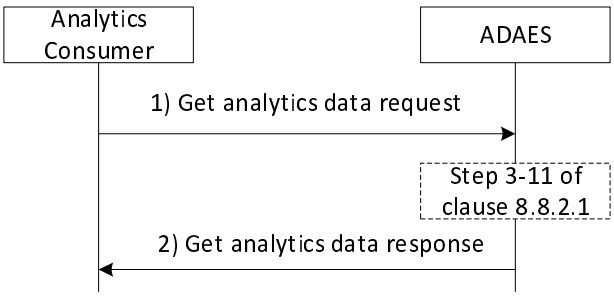

Figure 8.8.2.2-1: ADAES support for edge analytics

1. The analytics consumer sends a request message to the ADAE server to receive analytics data for one or more application servers. The request message includes the identity of the analytics consumer, security credential(s) for authorization and verification, identity of all the application server for which analytics data is requested, type of analytics data, time duration since when analytics data is required.

2. Upon receiving the request, the ADAE server authenticates and authorizes the analytics consumer. If the analytics consumer is authorized, the ADAE server may get the analytics by performing step 3 to 11 of clause 8.8.2.1. The ADAE server sends a response message including the statistical and predictive analytics of the edge performance/load for the edge platform or EES/EAS for the requested duration period (if the time duration is available).

8.8.3 Information flows

8.8.3.1 General

The following information flows are specified for edge load analytics based on 8.8.2.

8.8.3.2 Edge analytics subscription request

Table 8.8.3.2-1 describes information elements for the edge analytics subscription request from the VAL server / Consumer to the ADAE server.

Table 8.8.3.2-1: Edge analytics subscription request

Information element	Status	Description
Analytics Consumer ID	M	The identifier of the analytics consumer (VAL server, EAS).
Analytics ID	M	The identifier of the analytics event. This ID can be for example “Edge platform analytics”, “EES analytics”, “EAS analytics”.
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions.
Destination EAS information	O (NOTE)	This identifier shows the destination EAS information including destination EAS ID and destination EAS endpoint for which the analytics subscription applies.
Destination EES information	O (NOTE)	This identifier shows the destination EES information including destination EES ID and destination EES endpoint for which the analytics subscription applies.
DNN/DNAI	O (NOTE)	DNN or DNAIs information for which the subscription applies.
Target data producer profile criteria	O	Characteristics of the data producers to be used.
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction).
Area of Interest	O	The geographical or service area for which the subscription request applies.
Time validity	O	The time validity of the subscription request.
Reporting requirements	O	It describes the requirements for analytics reporting. This requirement may include e.g. the type and frequency of reporting (periodic or event triggered), the reporting periodicity in case of periodic, and reporting thresholds.
NOTE: At least one of these shall be present.		

8.8.3.3 Edge analytics subscription response

Table 8.8.3.3-1 describes information elements for the edge analytics subscription response from the ADAE server to the consumer.

Table 8.8.3.3-1: Edge analytics subscription response

Information element	Status	Description
Result	M	The result of the analytics subscription request (positive or negative acknowledgement).

8.8.3.4 Edge data collection subscription request

Table 8.8.3.4-1 describes information elements for the edge data collection subscription request from the ADAE server to the Data Producer at the EDN or the A-DCCF, or from ADAE server to ADAE client.

Table 8.8.3.4-1: Data collection subscription request

Information element	Status	Description
ADAE server ID	M	The identifier of the ADAE server
Data Collection Event ID	M	The identifier of the data collection event
Data Collection requirements	M	The requirements for data collection, including the format of data, frequency of reporting, level of abstraction of data, level of accuracy of data.
Analytics ID	O	The identifier of the analytics event, for which the data collection is needed.
List of Data Producer IDs	O	In case when this request is performed via A-DCCF, then the list of Data Producer IDs is needed.
Destination EAS information	O (NOTE)	This identifier shows the destination EAS information including destination EAS ID and destination EAS endpoint for which the analytics subscription applies.
Destination EES information	O (NOTE)	This identifier shows the destination EES information including destination EES ID and destination EES endpoint for which the analytics subscription applies.
DNN/DNAI	O (NOTE)	DNN or DNAIs information for which the subscription applies.
Target data producer profile criteria	O	Characteristics of the data producers to be used.
Area of Interest	O	The geographical or service area for which the requirement request applies.
Time validity	O	The time validity of the request.
NOTE: At least one of these shall be present.		

8.8.3.5 Edge data collection subscription response

Table 8.8.3.5-1 describes information elements for the Data collection subscription response from the edge Data Producer at the EDN or the A-DCCF to the ADAE server, or from ADAE client to ADAE server.

Table 8.8.3.5-1: Data collection subscription response

Information element	Status	Description
Result	M	The result of the edge data collection subscription request (positive or negative acknowledgement).

8.8.3.6 Data Notification

Table 8.8.3.6-1 describes information elements for the Data Notification from the Data Producer to the ADAE server.

Table 8.8.3.6-1: Data notification

Information element	Status	Description
Data Collection Event ID	M	The identifier of the data collection event.
Data Producer ID	M	The identity of Data Producer.
Destination EAS information	O (NOTE)	This identifier shows the destination EAS information including destination EAS ID and destination EAS endpoint for which the analytics subscription applies.
Destination EES information	O (NOTE)	This identifier shows the destination EES information including destination EES ID and destination EES endpoint for which the analytics subscription applies.
DNN/DNAI	O (NOTE)	DNN or DNAIs information for which the subscription applies.
Analytics ID	O	The identifier of the analytics event.
Data Type	M	The type of reported data samples which can be network data, application data, edge data, or different granularities / abstraction of data (e.g. real time, non-real time). This also indicates whether data are offline (from A-ADRF or not).
Data Output	M	The reported data, which can be inform of measurements or offline/historical data on the requested parameter based on subscription. Such data can be per EDN or per DNAI or per EAS/EES load statistics and edge computational resource utilization stats for a given time and area of interest.
NOTE: At least one of these shall be present based on the data collection event.		

8.8.3.7 Edge analytics Notification

Table 8.8.3.7-1 describes information elements for the Edge analytics Notification from the ADAE server to the VAL server / Consumer.

Table 8.8.3.7-1: Edge analytics notification

Information element	Status	Description
Analytics ID	M	The identifier of the analytics event.
Analytics Output	M	The analytics outputs, which can be predictive or statistical parameter.
> Edge platform analytics	O (see NOTE)	Statistics/predictions of the performance/load of the EDN or the associated edge platform, such as the number of EAS or EES connections.
>> Applicable time period	O	The time period that the analytics applies to.
>> Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
> EES analytics	O (see NOTE)	Statistics/predictions of the performance/load of the EES, such as the EES unavailability.
>> Applicable time period	O	The time period that the analytics applies to.
>> Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
> EAS analytics	O (see NOTE)	Statistics/predictions of the performance/load of the EAS, such as the EAS unavailability.
>> Applicable time period	O	The time period that the analytics applies to.
>> Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
NOTE: At least one of these information elements shall be provided based on the analytics ID specified in the edge analytics subscription request as in Table 8.8.3.2-1.		

8.8.3.8 Get analytics data request

Table 8.8.3.8-1 describes information elements for the Get analytics data request from the analytics consumer to the ADAE server.

Table 8.8.3.8-1: Get analytics data request

Information element	Status	Description
Analytics Consumer ID	M	The identifier of the analytics consumer (VAL server, EAS, EES).
Analytics ID	M	The identifier of the analytics event. This ID can be for example “Edge platform analytics”, “EES analytics”, “EAS analytics”.
Analytics type	M	The type of analytics, e.g. statistics or predictions.
Destination EASs information	O (NOTE)	This identifier provides the list of destination EASs information including destination EAS ID and destination EAS endpoint for which the analytics request applies.
Destination EESs information	O (NOTE)	This identifier provides the list of destination EESs information including destination EES ID and destination EES endpoint for which the analytics request applies.
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction).
Time duration	O	Time duration since when analytics data is required.
NOTE: At least one of these shall be present		

8.8.3.9 Get analytics data response

Table 8.8.3.9-1 describes information elements for the Get analytics data response from the ADAE server to the consumer.

Table 8.8.3.9-1: Get analytics data response

Information element	Status	Description
Result	M	The result of the analytics data request (positive or negative acknowledgement).
Analytics ID	O	The identifier of the analytics event.
Analytics Output	O	The analytics outputs, which can be predictive or statistical parameter.
> Edge platform analytics	O (see NOTE)	Statistics/predictions of the performance/load of the EDN or the associated edge platform, such as the number of EAS or EES connections.
>> Applicable time period	O	The time period that the analytics applies to.
>> Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
> EES analytics	O (see NOTE)	Statistics/predictions of the performance/load of the EES, such as the EES unavailability.
>> Applicable time period	O	The time period that the analytics applies to.
>> Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
> EAS analytics	O (see NOTE)	Statistics/predictions of the performance/load of the EAS, such as the EAS unavailability.
>> Applicable time period	O	The time period that the analytics applies to.
>> Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
NOTE: At least one of these information elements shall be provided based on the analytics ID specified in the get analytics data request as in Table 8.8.3.8-1.		

8.9 Procedure on Service experience to support application performance analytics

8.9.1 General

When Application server (like VAL server) is not available to provide analytics data due to overload or any other reasons or the application server is not providing the required quality of service experience at the UE side, the ADAE server may need to rely on alternate information sources like the application clients (like VAL clients) that provide the visibility on application service status. ADAE server can use this information from the clients alone, for the predictions and share with the consumer of the analytics. This clause provides a mechanism for the ADAE client to send service experience report to the ADAE server. ADAE server upon receiving the service experience information from the UE side entities can use it for predictions of application performance analytics.

NOTE: In this solution, if DDCC client is available in the UE, ADAE server uses data collection and reporting mechanisms as defined in 3GPP TS 26.531 [3], where the ADAE client acts as a UE application and ADAE server acts as an AF from Application service provider. The indirect reporting procedure (between ADAE client and ADAE server over ADAE-UU interface) may be used when a Direct Data Collection Client is not available in the UE.

8.9.2 Procedure

8.9.2.1 Push service experience information

The ADAE client determines the service experience information based on information received from the VAL client. The service experience information includes application specific performance measurements like end-to-end response time, connection bandwidth, request rate, server availability time, etc. On request from VAL client or any other trigger conditions, the ADAE client sends the service experience report about a VAL server to the ADAE server. The ADAE client may use the direct reporting mechanism as defined in clause 5.5 of 3GPP TS 26.531 [3]. The indirect reporting procedure (between ADAE client and ADAE server over ADAE-UU interface) may be used when a Direct Data Collection Client is not available in the UE or when the ADAE server (having Indirect Data Collection Client) needs to modify the collected UE data to satisfy the requirements of its data collection and reporting configuration. The information elements as defined in clause 8.9.3.1 are used by ADAE client to send the request and clause 8.9.3.2 are used by ADAE server to send the response.

For direct reporting, if data reporting session is not available, the ADAE client creates data reporting session as specified in clause 5.4 of 3GPP TS 26.531 [3]. Once data reporting session is available, the ADAE client (acting as a UE client) sends reports to ADAE server using direct reporting method as specified in clause 5.5 of 3GPP TS 26.531 [3].

For indirect reporting, Figure 8.9.2.1-1 illustrates the procedure where the ADAE client pushes the service experience information to the ADAE server.

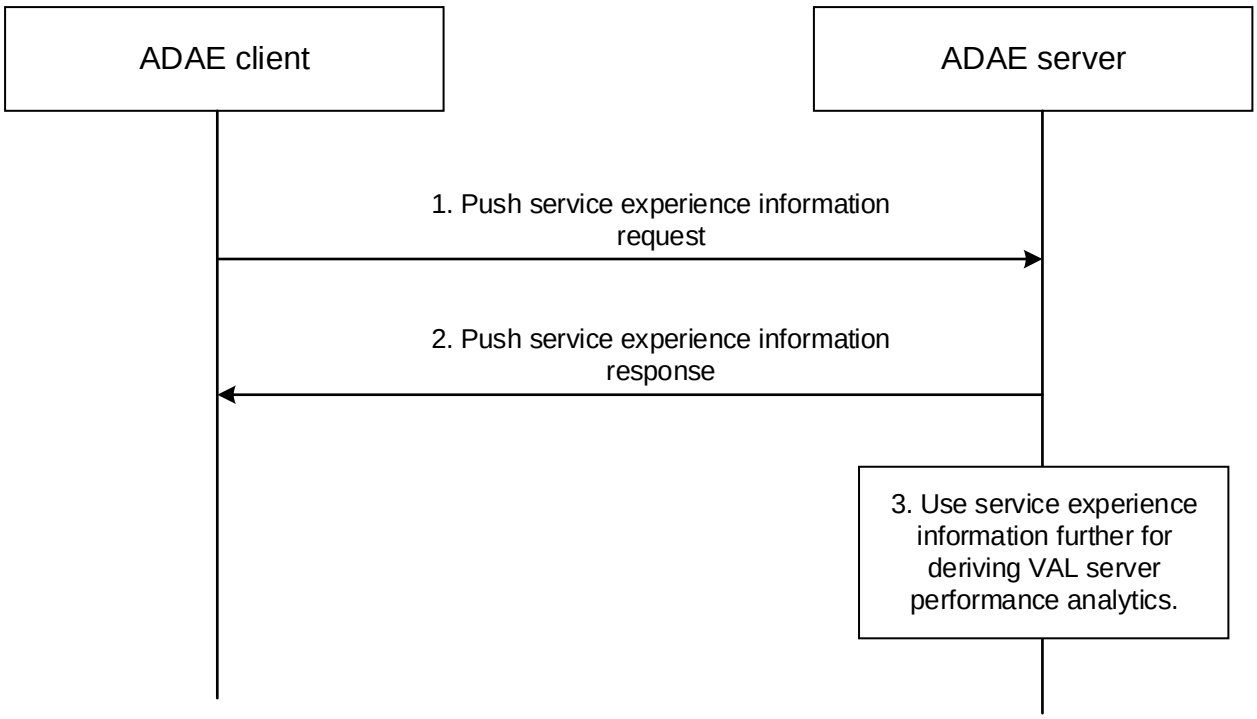

Figure 8.9.2.1-1: Push service experience informtion from UE

1. The ADAE client sends Push service experience request to the ADAE server. The request contains service experience report about a VAL server and includes the information elements as specified in Table 8.9.3.1-1.
2. The ADAE server sends Push service experience response to the ADAE client.
3. Upon receiving the Push service experience request from the ADAE client, the ADAE server uses the service experience report for derivation of VAL server performance analytics.

Once UE data is collected (either using direct reporting or indirect reporting), the ADAE server may take further actions based on the analysis of the report as shared by the ADAE client. A service experience information from certain UEs, can trigger the ADAE server to fetch further service experience information from other UEs. The ADAE server can use the service experience information report from other UEs to determine/predict analytics.

- If most of the UE side entities report similar service experience, then it could be the application server problem across globally.
- If only some UEs report a bad service experience, the problem could be localized among a group of UEs.
- If the bad service experience from only one UE, the problem is localized to the UE.

8.9.2.2 Pull service experience information

The procedure can be initiated by the ADAE server upon receiving a service experience from an ADAE client, to fetch service experience information from other ADAE clients or upon receiving VAL server performance analytics request from application service provider (application server) or any other event that requires the ADAE server to determine the service experience data.

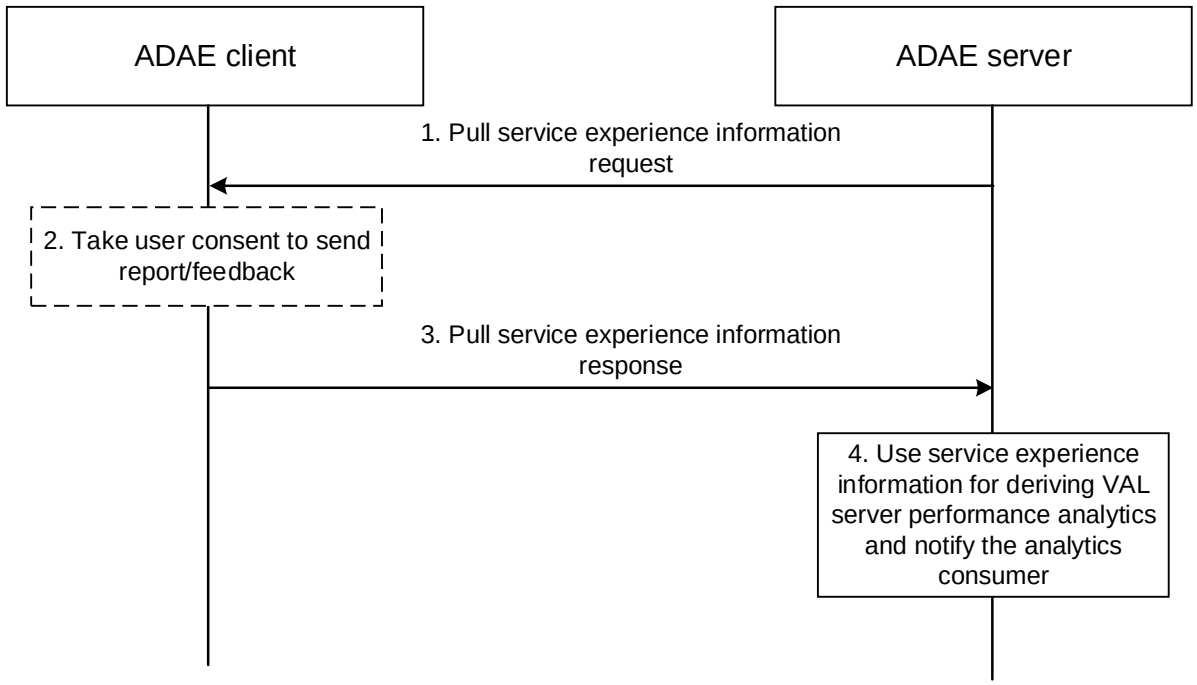

Figure 8.9.2.2-1: Pull service experience information from UE

1. The ADAE server sends Pull service experience information request to the ADAE client. The request contains identifier of the specific VAL server and VAL service ID, for which the service experience report is required, as mentioned in Table 8.9.3.3-1.
2. Upon receiving the Pull service experience information request from the ADAE server, the ADAE client may take user consent to send the report if the user consent is not available already.
3. The ADAE client sends the Pull service experience information response to the ADAE server. The ADAE client instructs the Direct Data Collection Client to prioritise immediate delivery of a UE data report to the Data Collection AF as specified in clause 5.5 of 3GPP TS 26.531 [3]. The service experience contains parameters as specified in Table 8.9.3.4-1.
4. The ADAE server uses the service experience report for derivation of VAL server performance analytics.

8.9.2.3 Service experience information based on triggers

The ADAE server configures triggers to the ADAE client to send the service experience report using the mechanism defined in clause 5.4 of 3GPP TS 26.531 [3].

The procedure can be initiated by the ADAE server upon receiving VAL server performance analytics request from application service provider (application server). The information elements as defined in clause 8.9.3.5 are used by ADAE server to send the request and clause 8.9.3.6 are used by ADAE client to send the response.

8.9.3 Information flows

8.9.3.1 Push service experience information request

Table 8.9.3.1-1 describes information elements for the Push service experience information request from the ADAE client to the ADAE server.

Table 8.9.3.1-1: Push service experience information request

Information element	Status	Description
VAL UE ID	M	The identifier of the VAL UE.
VAL service ID	O	The identifier of the VAL service for which the service experience report applies.
VAL server ID	M	The identifier of the VAL server for which the service experience report is sent.
Timestamp	O	Time stamp of the collected report.
VAL service experience report	O	Information related to VAL service experience. It may include end-to-end response time, connection bandwidth, request rate, VAL server availability, etc.

8.9.3.2 Push service experience information response

Table 8.9.3.2-1 describes information elements for the Push service experience information response from the ADAE server to the ADAE client.

Table 8.9.3.2-1: Push service experience information response

Information element	Status	Description
Result	M	Indicates success or failure of the request.

8.9.3.3 Pull service experience information request

Table 8.9.3.3-1 describes information elements for the Pull service experience information request from the ADAE server to the ADAE client.

Table 8.9.3.3-1: Pull service experience information request

Information element	Status	Description
VAL server ID	M	The identifier of the VAL server for which the service experience information is requested.
VAL service ID	O	The identifier of the VAL service for which the service experience information is requested.

8.9.3.4 Pull service experience information response

Table 8.9.3.4-1 describes information elements for the Pull service experience information response from the ADAE client to the ADAE server.

Table 8.9.3.4-1: Pull service experience information request response

Information element	Status	Description
Result	M	Indicates success or failure of the request.
VAL UE ID	M	The identifier of the VAL UE.
VAL service ID (NOTE)	O	The identifier of the VAL service for which the service experience report applies.
VAL Server ID	M	The identifier of the VAL server for which the service experience report is sent.
Timestamp (NOTE)	O	Time stamp of the collected report.
VAL service experience report (NOTE)	O	Information related to VAL service experience. It may include end-to-end response time, connection bandwidth, request rate, VAL server availability, etc.
NOTE: These IEs are included only if the result is success.		

8.9.3.5 Configure service experience report trigger request

Table 8.9.3.5-1 describes information elements for the Configure service experience report trigger request from the ADAE server to the ADAE client.

Table 8.9.3.5-1: Configure service experience report trigger request

Information element	Status	Description
VAL server specific criteria	M	List of VAL server specific criteria.
> VAL server ID	M	The identifier of the VAL server.
> Triggering Criteria	M	Information about the triggers on which the service experience is to be reported for the VAL server.
Common Triggering criteria	O	Information about the triggers (applicable to all VAL servers) on which the service experience is fetched.
Service experience measurement to monitor	O	Information about the service experience measurements which needs to be fetched and included in the report. If not present, by default end-to-end response time is measured.
Notification Target Address	O	The Notification target address (e.g. URL) where the notifications destined for the ADAE Server should be sent to.

8.9.3.6 Configure service experience report trigger response

Table 8.9.3.6-1 describes information elements for the Configure service experience report trigger response from the ADAE client to the ADAE server.

Table 8.9.3.6-1: Configure service experience report trigger response

Information element	Status	Description
Result	M	Indicates success or failure of the request.

8.10 Procedure on support for data storage

8.10.1 General

This clause describes procedures for supporting data storage to A-ADRF and remove stored date from the A-ADRF.

8.10.2 Procedure

8.10.2.1 Notification based data storage

Figure 8.10.2.1-1 illustrates the procedure for consumer to request A-ADRF to initiate request for data or analytics to store.

Pre-conditions:

1. Analytics or data consumer requests ADAE server, A-DCCF or data sources to store analytics or data to A-ADRF.
2. ADAE server, A-DCCF or A-ADRF are configured with default operator storage policies.

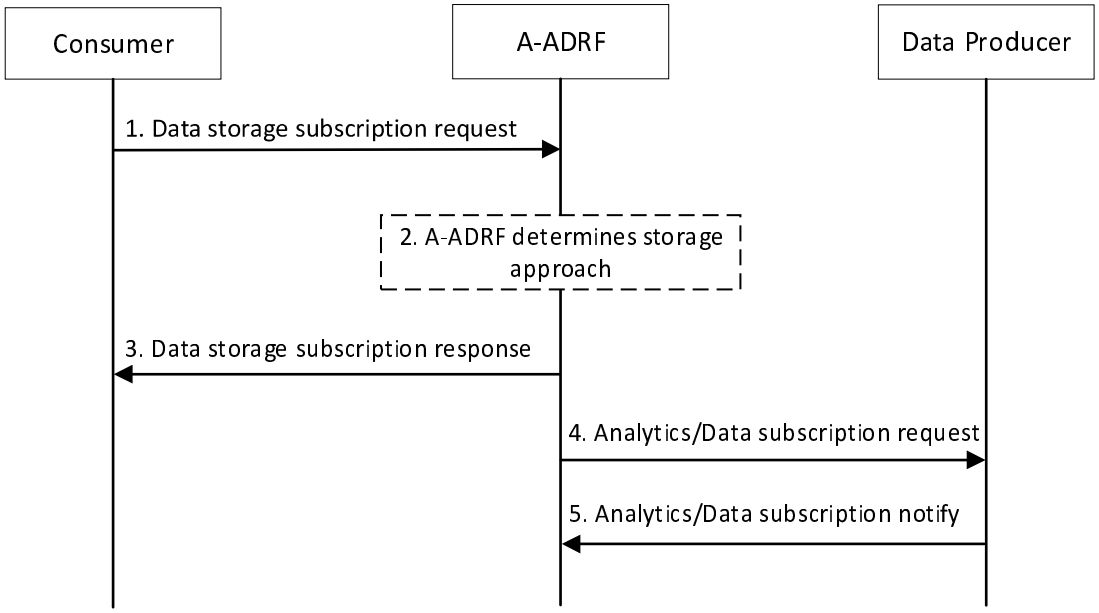

Figure 8.10.2.1-1: Support for data storage to A-ADRF

1. The consumer (A-DCCF or ADAE server) requests that the A-ADRF subscribes to Data Producer for receiving notifications. The determination may be made based on configuration or information supplied by the data or analytics. As specified in Table 8.10.3.2-1, the request to the A-ADRF specifies the data and/or analytics to which the A-ADRF will subscribe. The request includes identity of the consumer, security credential(s) for authorization and verification, and may include Storage Handling information (e.g. an expiration time for how long the data or analytics should be stored), indicate if a notification alerting the consumer needs to be sent prior to data deletion from the A-ADRF, notification endpoint information for use by the A-ADRF to send notifications (implicit subscription) alerting the consumer that data is about to be deleted, as specified in Table 8.10.3.2-1.

2. The A-ADRF may, based on implementation, determine whether the same data and/or analytics is already stored or being stored, based on the information sent in step 1 by the consumer. Based on Storage Handling information, the A-ADRF determines the Storage Approach (e.g. lifetime for the stored data and whether consumer is notified prior to data deletion).

3. If the data and/or analytics is already stored and/or being stored in the A-ADRF, the A-ADRF sends data storage subscription response message to the consumer indicating that data and/or analytics is stored. The storage subscription response includes the Storage Approach, as specified in Table 8.10.3.3-1.

4. The A-ADRF subscribes to the data producer (e.g. A-DCCF, ADAE server) to receive notifications with data or analytics, providing its notification endpoint address and a notification correlation ID.

5. The data producer sends data or analytics notifications containing the notification correlation ID provided by the A-ADRF to notification endpoint address. The analytics or data notifications shall contain timestamp. The ADRF stores the notifications.

8.10.2.2 Direct data storage

Figure 8.10.2.2-1 illustrates the procedure for the consumer to request A-ADRF for data or analytics storage.

Pre-conditions:

1. ADAE server or A-DCCF has data or analytics to be stored to A-ADRF.

2. ADAE server, A-DCCF or A-ADRF are configured with default operator storage policies.

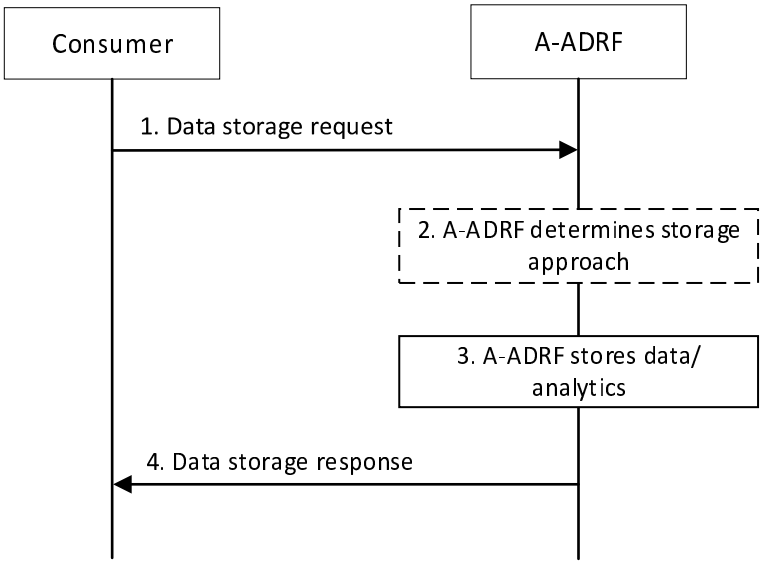

Figure 8.10.2.2-1: Support for data storage to A-ADRF

1. The consumer (e.g. ADAE server, A-DCCF) sends data storage request to the A-ADRF for storing data and/or analytics. The request message includes identity of the consumer, security credential(s) for authorization and verification, collected data with timestamp and/or analytics with timestamp, and may include Storage Handling information (e.g. a lifetime for how long the data or analytics should be stored), indicate if a notification alerting the consumer needs to be sent prior to data deletion from the A-ADRF, notification endpoint information for use by the A-ADRF to send notifications (implicit subscription) alerting the consumer that data is about to be deleted, as specified in Table 8.10.3.4-1.

2. Based on Storage Handling information (if available), the A-ADRF determines the Storage Approach (e.g. lifetime for storing data and whether consumer is notified prior to data deletion).

3. The A-ADRF stores the data and/or analytics sent by the consumer. The A-ADRF may, based on implementation, determine whether the same data and/or analytics is already stored or being stored based on the information sent in step 1 by the consumer and, if the same data and/or analytics is already stored or being stored in the A-ADRF, the A-ADRF decides to not store again the data and/or analytics sent by the consumer.

4. The ADRF sends data storage response message to the consumer indicating that data and/or analytics is stored, whether the A-ADRF determined at step 3 that data or analytics is already stored and the Storage Approach, as specified in Table 8.10.3.5-1.

8.10.2.3 Data removal from an A-ADRF

Figure 8.10.2.3-1 illustrates the procedure for the consumer to remove data previously stored in an A-ADRF, and for the A-ADRF to remove stored data with notification alerting to the consumer that data is about to be deleted.

Pre-conditions:

1. Case 1, A-ADRF Managing the Storage Approach: Consumer has data stored at the A-ADRF. The Storage Approach indicate that the consumer will be notified prior to data deletion, and the corresponding Data Deletion Notification Endpoint is known by the A-ADRF.

2. Case 2, Consumer Managing the Storage Approach: Consumer has data stored at the A-ADRF. The Storage Approach indicate that the consumer will not be notified prior to data deletion, or the corresponding Data Deletion Notification Endpoint is not known at the A-ADRF.

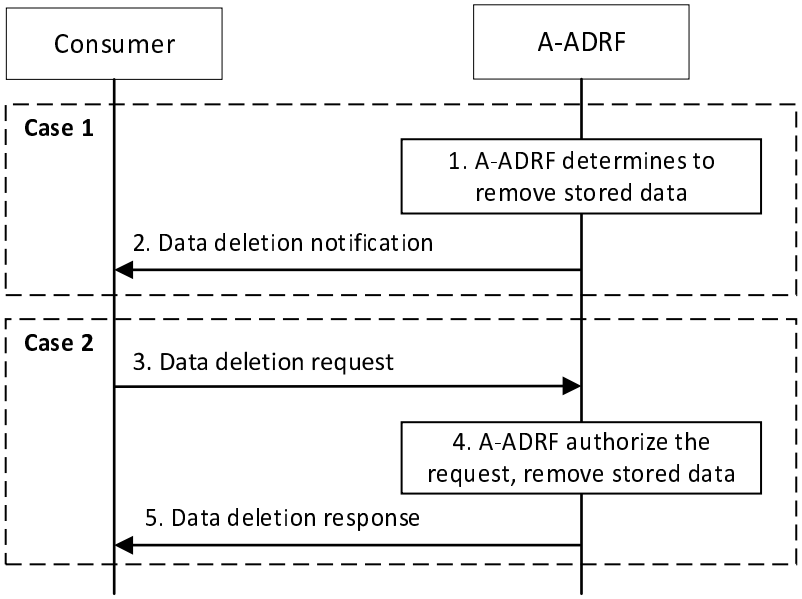

Figure 8.10.2.3-1: Support for data removal from A-ADRF

Conditional on A-ADRF Managing the Storage Approach (Case 1)

1. A-ADRF determines to remove data or analytics previously stored by a consumer (e.g. ADAE server, A-DCCF), as the lifetime of the stored data or analytics has expired (according to the Storage Approach).

2. If indicated by the Storage Approach, the A-ADRF sends a data deletion notification alerting the consumer that data is about to be deleted. The data deletion notification message includes Data or Analytics Deletion Alert, as specified in Table 8.10.3.6-1.

NOTE: This is an implicit subscription.Conditional on Consumer Managing the Storage Approach (Case 2)

3. The consumer (e.g. ADAE server, A-DCCF) determines that the data or analytics has to be deleted. The consumer sends data deletion request to the A-ADRF to remove specified data previously stored at the A-ADRF by the consumer. The request message includes the identifier(s) of the data set to be removed, as specified in Table 8.10.3.7-1.

4. The A-ADRF checks the relevant authorization for the request. If the authorization is successful, the A-ADRF deletes all copies of the stored data.

5. The A-ADRF sends data deletion response to the consumer. The response includes the deletion result (i.e. data deleted, data not found, data found but not deleted), as specified in Table 8.10.3.8-1.

8.10.3 Information flows

8.10.3.1 General

The following information flows are specified for data storage based on 8.10.2.

8.10.3.2 Data storage subscription request

Table 8.10.3.2-1 describes information elements for the data storage subscription request from the consumer (ADAE server, A-DCCF) to the A-ADRF.

Table 8.10.3.2-1: Data storage subscription request

Information element	Status	Description
Consumer ID	M	The identifier of the consumer (ADAE server, A-DCCF).
Data Producer ID	O	The identifier of the data producer (e.g. ADAE server, A-DCCF).
Analytics ID	O	The identifier of the analytics event. This IE shall be provided when Analytics Producer ID is present.
Analytics Type	O	The type of analytics for the event, which include category (e.g. statistics or predictive analytics), may include mode (e.g. offline or online) and indication on ML-enabled analytics. This IE shall be provided when Analytics Producer ID is present.
Target Data Producer Profile Criteria	O	Characteristics of the data producers to be used. This IE shall be provided when Data Producer ID is present.
Area of Interest	O	The geographical or service area for which the subscription request applies.
Time Validity	O	The time validity of the subscription request to the A-ADRF.
Storage Handling information	O	The information for storage handling.
> Lifetime	O	A lifetime for how long the data or analytics should be stored.
> Alert Indicator	O	To indicate that a notification alerting the consumer be sent prior to data deletion from the A-ADRF.
Data Deletion Notification Endpoint	O	Information of the notification endpoint, which is used by the A-ADRF to send data or analytics deletion alert.

8.10.3.3 Data storage subscription response

Table 8.10.3.3-1 describes information elements for the data storage subscription response from the A-ADRF to the consumer (ADAE server, A-DCCF).

Table 8.10.3.3-1: Data storage subscription response

Information element	Status	Description
Result	M	The result of the data storage subscription request (positive or negative acknowledgement).
Storage Approach	M	Represent the Storage Approach (e.g. lifetime for storing data, and whether consumer is notified prior to data deletion).

8.10.3.4 Data storage request

Table 8.10.3.4-1 describes information elements for the data storage request from the consumer (ADAE server, A-DCCF) to the A-ADRF.

Table 8.10.3.4-1: Data storage request

Information element	Status	Description
Consumer ID	M	The identifier of the consumer (ADAE server, A-DCCF).
Data Type	M	To indicate the data type (e.g. data or analytics).
Content	M	The data or analytics to be stored.
Timestamp	M	The timestamp of the data or analytics.
Analytics ID	O	The identifier of the analytics event. This IE shall be provided if the Storage Type is analytics.
Analytics Type	O	The type of analytics, which include category (e.g. statistics or predictive analytics), may include mode (e.g. offline or online) and indication on ML-enabled analytics. This IE shall be provided if the Data Type is analytics.
Data Source Information	O	Information of the data source. This IE shall be provided if the Data Type is data.
Storage Handling information	O	The information for storage handling.
> Lifetime	O	A lifetime for how long the data or analytics should be stored.
> Alert Indicator	O	To indicate that a notification alerting the consumer be sent prior to data deletion from the A-ADRF.
Data Deletion Notification Endpoint	O	Information of the notification endpoint, which is used by the A-ADRF to send data or analytics deletion alert.

8.10.3.5 Data storage response

Table 8.10.3.5-1 describes information elements for the data storage response from the A-ADRF to the consumer (ADAE server, A-DCCF).

Table 8.10.3.5-1: Data storage response

Information element	Status	Description
Result	M	The result of the data storage request (positive or negative acknowledgement).
Storage Approach	M	Represent the Storage Approach (e.g. lifetime for storing data, and whether consumer is notified prior to data deletion).

8.10.3.6 Data deletion notification

Table 8.10.3.6-1 describes information elements for the data deletion notification from the A-ADRF to the consumer (ADAE server, A-DCCF).

Table 8.10.3.6-1: Data deletion notification

Information element	Status	Description
Consumer ID	M	The identifier of the consumer (ADAE server, A-DCCF).
Data or Analytics Deletion Alert	M	Indicates that the stored data or analytics is about to be deleted.
Identifier(s) of data set	M	Identifier(s) of the data set to be deleted.

8.10.3.7 Data deletion request

Table 8.10.3.7-1 describes information elements for the data deletion request from the consumer (ADAE server, A-DCCF) to the A-ADRF.

Table 8.10.3.7-1: Data deletion request

Information element	Status	Description
Consumer ID	M	The identifier of the consumer (ADAE server, A-DCCF).
Identifier(s) of data set	M	Identifier(s) of the data set to be deleted.

8.10.3.8 Data deletion response

Table 8.10.3.8-1 describes information elements for the data deletion response from the A-ADRF to the consumer (ADAE server, A-DCCF).

Table 8.10.3.8-1: Data deletion response

Information element	Status	Description
Identifier(s) of data set	M	Identifier(s) of the data set.
Deletion result	M	The result of data deletion, i.e. data deleted, data not found, data found but not deleted.

8.11 Procedure for edge computing preparation analytics

8.11.1 General

This clause describes the procedure for edge computing preparation analytics.

8.11.2 Procedure

8.11.2.1 Subscribe-notify model

Figure 8.11.2.1-1 illustrates the procedure for edge computing preparation analytics.

Pre-conditions:

1. ADAES is connected to A-ADRF.
2. ADAES has subscribed to OAM for receiving management analytics.

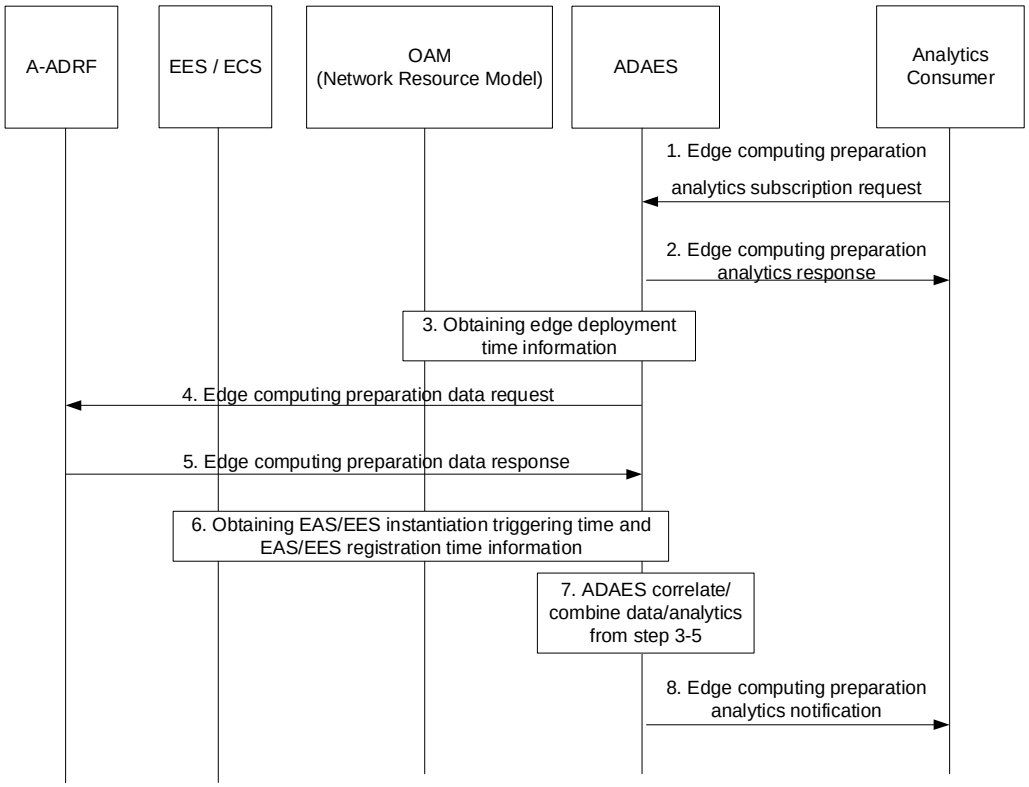

Figure 8.11.2.1-1: ADAES support for edge computing preparation analytics subscribe-notify model

1. The analytics consumer (e.g., VAL server, ECS, EES) of the ADAE server analytics service sends an Edge computing preparation analytics subscription request to the ADAE server.

2. The ADAE server sends an Edge computing preparation analytics response as an ACK to the analytics consumer.

3. The ADAE server utilizes OAM (Network Resource Model) for edge deployment time information for EAS, EES, or ECS. The deployment time information is determined from the Process Monitor that specifies, for instance, NOT_STARTED, RUNNING and start and/or end time for these states as described in 3GPP TS 28.623 [15].

4. The ADAE server requests historical edge deployment time information of EAS, EES, and/or ECS from A-ADRF by sending an Edge computing preparation data request.

5. Based on the request, the ADAE server receives historical edge deployment time information of EAS, EES, and/or ECS by receiving an Edge computing preparation data response from A-ADRF.

6. The ADAE server collects EAS and/or EES instantiation triggering time and their registration time from the corresponding EES/ECS to determine when the instantiation request is sent to OAM and when EAS/EES service is ready.

7. The ADAE server abstracts or correlates the data/analytics from step 3-6. Based on the request in step 1, ADAES may also provide predictions for the edge deployment time.

8. The ADAE server sends an Edge computing preparation analytics notification to the analytics consumer, based on the request and the derived analytics in step 7. Such analytics indicate analytics and/or prediction of the edge deployment time for EAS, EES, and/or ECS.

8.11.2.2 Request-response model

Figure 8.11.2.2-1 illustrates the procedure where the analytics consumer (e.g., VAL server, ECS, EES) requests edge computing preparation analytics using the request/response model.

Pre-conditions:

1. ADAES is connected to A-ADRF.
2. ADAES has subscribed to OAM for receiving management analytics.

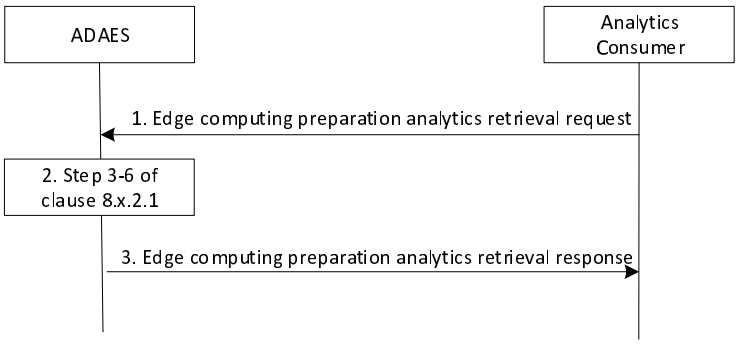

Figure 8.11.2.2-1: ADAES support for edge computing preparation analytics request/response model

1. The analytics consumer (e.g., VAL server, ECS, EES) sends an Edge computing preparation analytics retrieval request to the ADAES.
2. Upon receiving the request, the ADAE server authenticates and authorizes the analytics consumer. If the analytics consumer is authorized, the ADAES performs step 3-7 of clause 8.11.2.1.
3. The ADAES sends an Edge computing preparation analytics retrieval response to the analytics consumer.

8.11.3 Information flows

8.11.3.1 General

The following information flows are specified for edge computing preparation analytics based on 8.11.2.

8.11.3.2 Edge computing preparation analytics subscription request

Table 8.11.3.2-1 describes information elements for the edge computing preparation analytics subscription request from the analytics consumer (e.g., the VAL server, ECS, EES) to the ADAE server.

Table 8.11.3.2-1: Edge computing preparation analytics subscription request

Information element	Status	Description
Analytics Consumer ID	M	The identifier of the analytics consumer (VAL server, ECS etc.).
Analytics ID	O	The identifier of the analytics event. This ID can be for example "edge computing preparation analytics".
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions.
Reporting requirements	O	Requirements for analytics reporting. The requirements may include for example when the deployment information of the target (EAS, EES, ECS) is set to a specific state (such as "finished") or when the state is changed.
DNN/DNAI	O	DNN or DNAIs information of the EDN for which the subscription applies.
ECS provider ID	O	The identifier of the ECS provider
ECS endpoint	O	By providing the ECS endpoint, the consumer wants to subscribe to the EES instantiation info (EESs that will register in the ECS)
EES provider ID	O	The identifier of the EES provider
EES endpoint	O	By providing the EES endpoint, the consumer wants to subscribe to the EAS instantiation info (EASs that will register in the EES)
EAS provider ID	O	The identifier of the EAS provider
EAS ID	O	Identifies an EAS service.
EAS/EES/ECS resource requirements	O	The resources (i.e. available compute, graphical compute, memory, storage) needed for EAS/EES/ECS as described in Table 8.2.5-1 in 3GPP TS 23.558 [14].
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction).
Area of Interest	O	The geographical or service area for which the requirement request applies.
Time validity	O	The time validity of the subscription request.

8.11.3.3 Edge computing preparation analytics subscription response

Table 8.11.3.3-1 describes information elements for the edge computing analytics preparation analytics subscription response from the ADAE server to the analytics consumer.

Table 8.11.3.3-1: Edge computing preparation analytics subscription response

Information element	Status	Description
Result	M	The result of the analytics subscription request (positive or negative acknowledgement).

8.11.3.4 Edge computing preparation analytics notification

Table 8.11.3.4-1 describes information elements for the edge computing preparation analytics notification from the ADAE server to the analytics consumer.

Table 8.11.3.4-1: Edge computing preparation analytics notification

Information element	Status	Description
Analytics ID	O	The identifier of the analytics event.
Analytics Output	M	Represents the analytics output including prediction or statistics for the EAS/EES/ECS deployment time.
Confidence level	O	For predictive analytics, the achieved confidence level can be provided.

8.11.3.5 Edge computing preparation data request

Table 8.11.3.5-1 describes information elements for the edge computing preparation data request from the ADAE server to the A-ADRF/EES/ECS.

Table 8.11.3.5-1: Edge computing preparation data request

Information element	Status	Description
ADAE server ID	M	The identifier of the ADAE server.
Analytics ID	M	The identifier of the analytics event.
Target ECS information	O (NOTE)	This identifier shows the target ECS information
Target EES information	O (NOTE)	This identifier shows the target EES information
Target EAS information	O (NOTE)	This identifier shows the target EAS information
Time validity	O	The time validity of the request.
NOTE: At least one of these shall be present for A-ADRF as receiver. Target ECS information is included for collecting EES instantiation triggering time and EES registration time. Target EES information is included for collecting EAS instantiation triggering time and EAS registration time.		

8.11.3.6 Edge computing preparation data response

Table 8.11.3.6-1 describes information elements for the edge computing preparation data response from the A-ADRF/EES/ECS to the ADAE server.

Table 8.11.3.6-1: Edge computing preparation data response

Information element	Status	Description
Analytics ID	M	The identifier of the analytics event.
Data Type	M	The type of reported data samples which can be network data, application data, edge data, or different granularities / abstraction of data (e.g., real time, non-real time).
Data Output	M	The reported data, which can be in form of measurements or offline/historical data on the requested parameter based on the request. The reported data includes historical ECS/EES/EAS deployment time information, EES/EAS registration data etc.

8.11.3.7 Edge computing preparation analytics retrieval request

Table 8.11.3.7-1 describes information elements for the Edge computing preparation analytics retrieval request from the analytics consumer to the ADAE server.

Table 8.11.3.7-1: Edge computing preparation analytics retrieval request

Information element	Status	Description
Analytics Consumer ID	M	The identifier of the analytics consumer (VAL server, ECS etc.).
Analytics ID	O	The identifier of the analytics event. This ID can be for example “edge computing preparation analytics”.
Analytics type	M	Whether analytics event is about prediction or statistics.
DNN/DNAI	O	DNN or DNAIs information of the EDN for which the subscription applies.
ECS provider ID	O	The identifier of the ECS provider
ECS endpoint	O	By providing the ECS endpoint, the consumer wants to subscribe to the EES instantiation info (EESs that will register in the ECS)
EES provider ID	O	The identifier of the EES provider
EES endpoint	O	By providing the EES endpoint, the consumer wants to subscribe to the EAS instantiation info (EASs that will register in the EES)
EAS provider ID	O	The identifier of the EAS provider
EAS ID	O	Identifies an EAS service.
EAS/EES/ECS resource requirements	O	The resources (i.e. available compute, graphical compute, memory, storage) needed for EAS/EES/ECS as described in Table 8.2.5-1 in 3GPP TS 23.558 [14].
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction).
Area of Interest	O	The geographical or service area for which the requirement request applies.
Time duration	O	Time duration since when analytics data is required.

8.11.3.8 Edge computing preparation analytics retrieval response

Table 8.11.3.8-1 describes information elements for the Edge computing preparation analytics retrieval response from the ADAE server to the analytics consumer.

Table 8.11.3.8-1: Edge computing preparation analytics retrieval response

Information element	Status	Description
Results	M	The result of the analytics data request (positive or negative acknowledgement).
Analytics ID	O	The identifier of the analytics event.
Analytics Output	M	Represents the analytics output including prediction or statistics for the EAS/EES/ECS deployment time.
Confidence level	O	For predictive analytics, the achieved confidence level can be provided.

8.12 Procedure for supporting data collection to A-DCCF

8.12.1 General

This clause describes two procedures (covering both subscribe-notify and request-response models in 8.12.2.1 and 8.12.2.2 respectively) for supporting data collection at A-DCCF.

8.12.2 Procedure

8.12.2.1 Subscribe-notify model

Figure 8.12.2.1-1 illustrates the procedure for consumer to request A-DCCF to initiate subscription for data or analytics collection. The procedure may be utilized by the consumer to update the subscription for data or analytics collection.

Pre-conditions:

1. Consumer (ADAE server) collects data or analytics via A-DCCF from data producer.

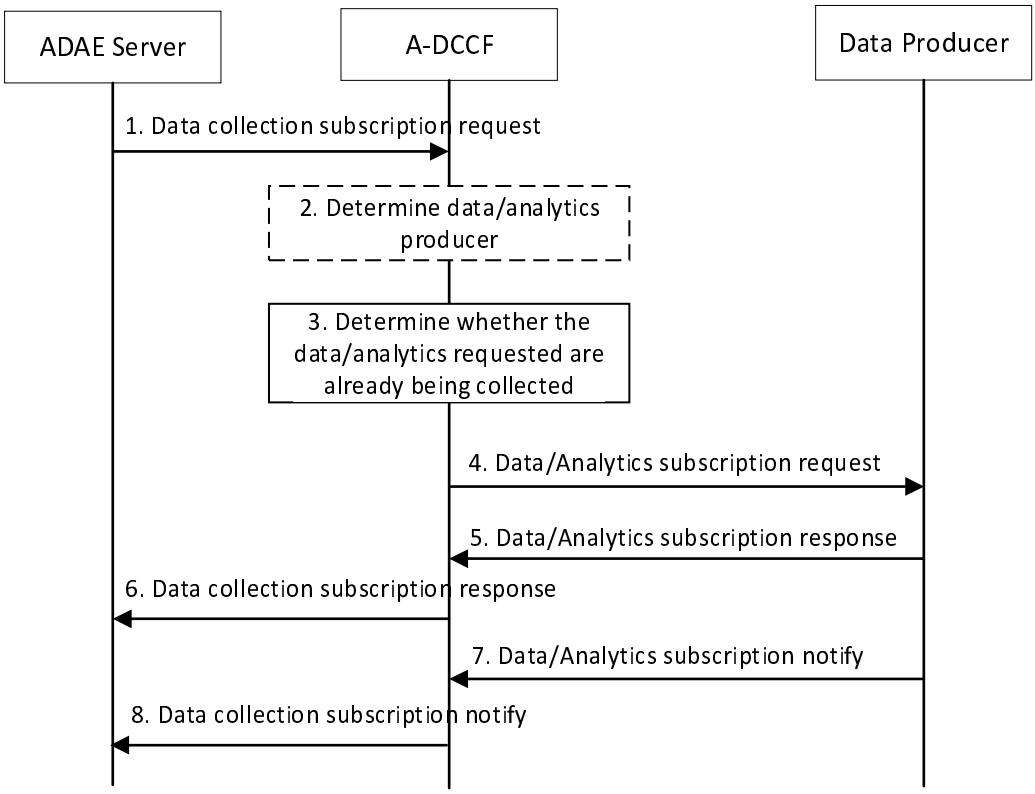

Figure 8.12.2.1-1: Support for data collection over A-DCCF

1. The consumer (ADAE server) sends a data collection subscription request to A-DCCF for collecting data/analytics. As specified in Table 8.12.3.2-1, the request message includes identifier of the consumer (ADAE server ID), Data Collection Event ID, and Data Collection Requirements. The request message may include the identifier of Data Producer, Analytics ID, target data producer profile criteria, process requirements, Area of Interest, Time validity, storage requirements, and notification endpoints. The consumer decides to go via A-DCCF based on internal configuration.

2. If the data producer is not identified by the consumer, the A-DCCF determines the data procedure that can provide data/analytics. If the consumer requested storage of data/analytics in an A-ADRF but the A-ADRF ID is not provided by the consumer, or the collected data/analytics is to be stored in an A-ADRF according to configuration on the A-DCCF, the A-DCCF selects an A-ADRF to store the collected data/analytics.

3. The A-DCCF determines whether the data/analytics requested in step 1 are already being collected. If the requested data/analytics are already being collected by a consumer, the A-DCCF adds the new consumer to the list of consumers that are subscribed for these data/analytics.

4. If the data/analytics subscribed in step 1 is not being collected by the A-DCCF, the A-DCCF subscribes to the data producer for data/analytics.

   If the data/analytics subscribed in step 1 partially matches the data/analytics that is already being collected by the A-DCCF, a modification of this subscription to the data producer would satisfy both the existing data/analytics subscriptions as well as the newly requested data/analytics, the A-DCCF requests an update of the previous

subscription to the data producer. The A-DCCF adds the consumer to the list of consumers that are subscribed for these data/analytics.

5. Upon received the data/analytics subscription request from the A-DCCF, the data producer determines whether the required data/analytics can be provided and sends data/analytics subscription response to the A-DCCF.

6. The A-DCCF sends data/analytics subscription response to the consumer.

7. When the required data/analytics are available, the data producer notifies the data/analytics to the A-DCCF.

8. The A-DCCF notifies the data/analytics to all notification endpoints indicated in step 1. Data/analytics sent to notification endpoints may be processed by the DCCF upon to the request in step 1. The DCCF may store the data/analytics in the A-ADRF if requested by the consumer or if required by A-DCCF configuration.

8.12.2.2 Request-response model

Figure 8.12.2.2-1 illustrates the procedure for the consumer to request A-DCCF for data or analytics collection.

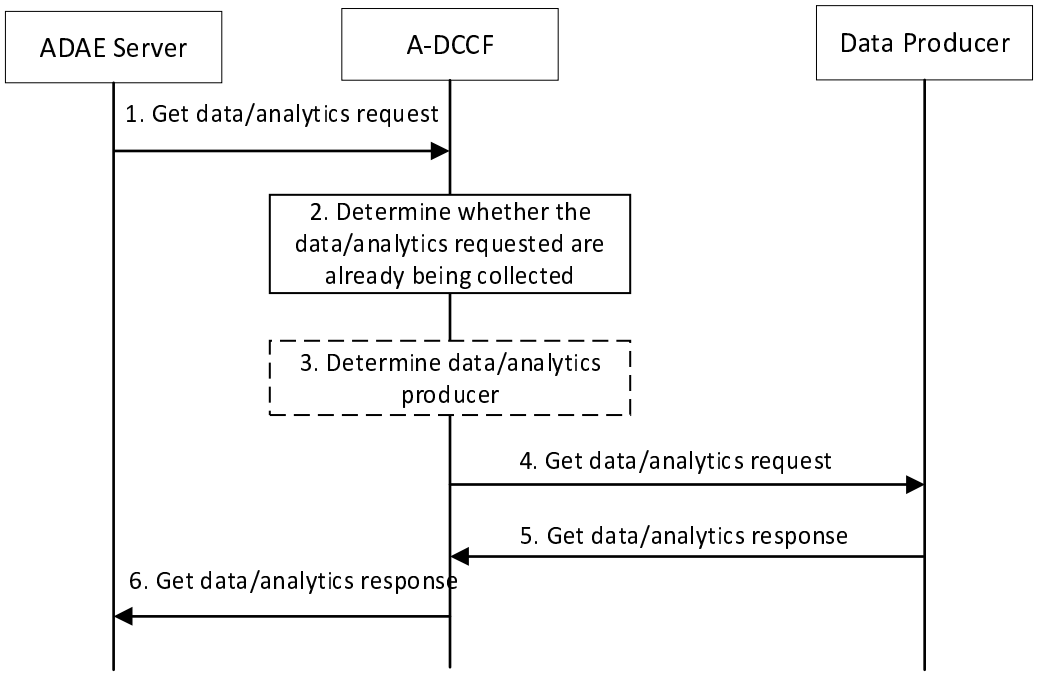

Figure 8.12.2.2-1: Support for Get data/analytics over A-DCCF

1. The consumer (ADAE server) sends a Get data/analytics request to A-DCCF for data/analytics collection. As specified in Table 8.12.3.5-1, the request message includes identifier of the consumer (ADAE server ID), and Data/Analytics Requirements. The request message may include the identifier of Data Producer, Analytics ID, target data producer profile criteria, process requirements, storage requirements, and notification endpoints. The consumer decides to go via A-DCCF based on internal configuration.

2. The A-DCCF determines whether the data/analytics requested in step 1 are already being collected. If the requested data/analytics are already being collected by a consumer, the A-DCCF adds the new consumer to the list of consumers that are subscribed for these data/analytics.

3. If the data/analytics requested in step 1 is not being collected by the A-DCCF, and the data producer is not identified by the consumer, the A-DCCF determines the data procedure that can provide data/analytics. If the consumer requested storage of data/analytics in an A-ADRF but the A-ADRF ID is not provided by the consumer, or the collected data/analytics is to be stored in an A-ADRF according to configuration on the A-DCCF, the A-DCCF selects an A-ADRF to store the collected data/analytics.

4. The A-DCCF sends Get data/analytics request to the data producer for data/analytics.

5. Upon received the data/analytics request from the A-DCCF, the data producer determines whether the required data/analytics can be provided and sends data/analytics response to the A-DCCF. The required data/analytics may be contained in the response if they are available at the data producer.

6. The A-DCCF sends data/analytics response to the consumer. The required data/analytics may be contained in the response if get from the data producer.

8.12.3 Information flows

8.12.3.1 General

The following information flows are specified for data collection based on clause 8.12.2.

8.12.3.2 Data collection subscription request

Table 8.12.3.2-1 describes information elements for the data collection subscription request from the consumer (ADAE server) to the A-DCCF.

Table 8.12.3.2-1: Data collection subscription request

Information element	Status	Description
Consumer ID	M	The identifier of the consumer (ADAE server ID).
Data Collection Event ID	M	The identifier of the data collection event.
Data Collection requirements	M	The requirements for data collection, including the format of data, frequency of reporting, level of abstraction of data, level of accuracy of data.
Analytics ID	O	The identifier of the analytics event, for which the data collection is needed.
List of Data Producer IDs	O	The list of Data Producer IDs.
Target data producer profile criteria	O	Characteristics of the data producers to be used.
Area of Interest	O	The geographical or service area for which the requirement request applies
Time validity	O	The time validity of the request
Process requirements	O	Requirements on processing the collected data/analytics.
Storage requirements	O	Requirements on storage of the collected data/analytics.
> A-ADRF ID	O	The identifier of A-ADRF for store the collected data/analytics.
Notification endpoints ID or address	O	The identifier or address of the notification endpoints.

8.12.3.3 Data collection subscription response

Table 8.12.3.3-1 describes information elements for the data collection subscription response from the A-DCCF to the consumer (ADAE server).

Table 8.12.3.3-1: Data collection subscription response

Information element	Status	Description
Result	M	The result of the data collection subscription request (positive or negative acknowledgement).

8.12.3.4 Data collection notification

Table 8.12.3.4-1 describes information elements for the data collection notification from the A-DCCF to the consumer (ADAE server).

Table 8.12.3.4-1: Data collection notification

Information element	Status	Description
Data Collection Event ID	M	The identifier of the data collection event.
Analytics ID	O	The identifier of the analytics event.
Analytics Type	O	The type of reported analytics, which can be statistics, prediction, etc.
Data Type	O	The type of reported data samples, which can be UE data, network data, application data, edge data, or different granularities/abstraction of data (e.g. real time, non-real time).
Data Output	M	The reported data/analytics, which can be inform of measurements or offline/historical data/analytics based on subscription.
Process information	O	Information of the processing of the collected data/analytics.
Storage information	O	Information of the storage of the collected data/analytics.
> A-ADRF ID	O	The identifier of A-ADRF for store the collected data/analytics.

8.12.3.5 Get Data/Analytics request

Table 8.12.3.5-1 describes information elements for the Get data/analytics request from the consumer (ADAE server) to the A-DCCF.

Table 8.12.3.5-1: Get Data/Analytics request

Information element	Status	Description
Consumer ID	M	The identifier of the consumer (ADAE server ID).
Data/Analytics requirements	M	The requirements for data/analytics collection, including the format of data, level of abstraction of data, level of accuracy of data.
Analytics ID	O	The identifier of the analytics event for the required analytics.
List of Data Producer IDs	O	The list of Data Producer IDs.
Target data producer profile criteria	O	Characteristics of the data producers to be used.
Area of Interest	O	The geographical or service area for which the requirement request applies
Time validity	O	The time validity of the request
Process requirements	O	Requirements on processing the collected data/analytics.
Storage requirements	O	Requirements on storage of the collected data/analytics.
> A-ADRF ID	O	The identifier of A-ADRF for store the collected data/analytics.
Notification endpoints ID or address	O	The identifier or address of the notification endpoints.

8.12.3.6 Data collection response

Table 8.12.3.6-1 describes information elements for the data collection response from the A-DCCF to the consumer (ADAE server).

Table 8.12.3.6-1: Data collection response

Information element	Status	Description
Result	M	The result of the analytics data request (positive or negative acknowledgement).
Analytics ID	O	The identifier of the analytics event.
Analytics Type	O	The type of reported analytics, which can be statistics, prediction, etc.
Data Type	O	The type of reported data samples, which can be UE data, network data, application data, edge data, or different granularities/abstraction of data (e.g. real time, non-real time).
Data Output	M	The reported data/analytics, which can be inform of measurements or offline/historical data/analytics based on subscription.
Process information	O	Information of the processing of the collected data/analytics.
Storage information	O	Information of the storage of the collected data/analytics.
> A-ADRF ID	O	The identifier of A-ADRF for store the collected data/analytics.

8.12.3.7 Data producer profile

The data producer profile IE includes information about the data generation/production capability of the data producer to support data collection for data analytics service and the availability/accessibility of the generated/produced data, as defined in Table 8.12.3.7-1.

Table 8.12.3.7-1: Data producer profile

Information element	Status	Description
Data Producer ID	M	ID of the data producer.
Data producer type (NOTE)	M	Specifies the type of the data producer, e.g., ADAEC, A-DCCF, A-ADRF, VAL server, SEAL server, SEAL client, EES, EAS.
Data type (NOTE)	M	Type of information that can be provided by the data producer, e.g., performance indicators, reproducer usage data, server load data, application performance, edge load.
Data producer role (NOTE)	O	Role of the data producer, e.g., generating entity, original producer, repository.
Original producer ID (NOTE)	O	If the data producer role is not “original producer” or “generating entity”, specifies the Producer ID of the original data producer for the data provided by this data producer. If the data producer type is A-DCCF, this is a list of Data Producer IDs.
Data freshness (NOTE)	O	If the data producer role is not “original producer” or “generating entity”, length of time elapsed after the data is generated until is available at the data producer. Alternatively, the data collection rate supported by the producer is provided.
Data producer capability (NOTE)	O	Indicates data producer capabilities for this data type, e.g. how long the data can be stored, support for anonymization, data generation rate and schedule.
NOTE: When the Data producer profile IE is used for Target data producer profile criteria (e.g. Table 8.12.3.2-1 and Table 8.12.3.5-1), this IE may be a list of values.		

8.13 Procedure on support for server-to-server performance analytics

8.13.1 General

This clause describes the procedure for server-to-server performance analytics.

8.13.2 Procedure

Figure 8.13.2.1-1 illustrates the procedure for server-to-server performance analytics.

Pre-conditions:

1. ADAES is connected to A-ADRF and the target server (server#1).

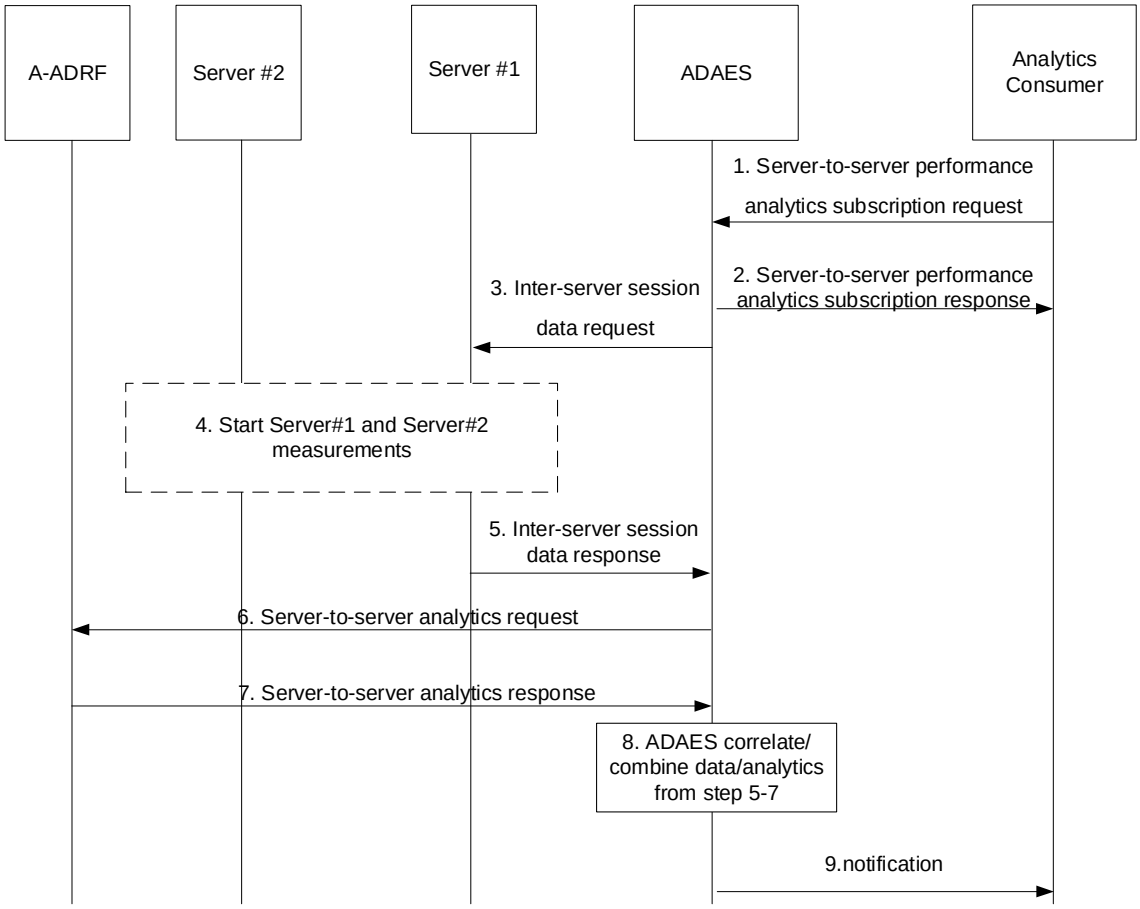

Figure 8.13.2.1-1: ADAES support for server-to-server performance analytics

1. The analytics consumer (e.g., VAL server, EES) of the ADAE server analytics service sends a server-to-server analytics subscription request to the ADAE server. Such request can include whether the analytics notification shall be periodic or based on an expected application QoS change (in that case also the thresholds can be provided at the request)

2. The ADAE server sends a server-to-server analytics subscription response as an ACK to the analytics consumer.

3. The ADAE server identifies server#1 where the session performance analytics need to be performed. The ADAES server sends an Inter-server data request to server #1. Such request includes QoS attributes to be analysed (latency, bitrate, jitter, application layer PER) based on the request in step 1.

4. Bases on the request, measurement may be started between the server#1 and server#2. Such data can be about the latency, throughput, jitter, QoE measurements, PQI load, etc.

NOTE: How the measurement is collected is out of 3GPP scope. The measurement data can be already available in server#1 or server#2.

5. Server#1 sends the analytics to the ADAE server in an Inter-server data response message.

6. The ADAE server requests historical inter-server performance analytics from A-ADRF by sending a Server-to-server analytics request.

7. Based on the request, the ADAE server receives historical inter-server performance analytics by receiving a Server-to-server analytics response from A-ADRF.

8. The ADAE server abstracts or correlates the data/analytics from step 5-7. Based on the request in step 1, ADAES may also provide predictions for performance change.

9. The ADAE server sends a server-to-server analytics notification to the analytics consumer.

8.13.3 Information flows

8.13.3.1 General

The following information flows are specified for server-to-server performance analytics based on 8.13.2.

8.13.3.2 Server-to-server performance analytics subscription request

Table 8.13.3.2-1 describes information elements for the server-to-server performance analytics subscription request from the analytics consumer (e.g., the VAL server, EES) to the ADAE server.

Table 8.13.3.2-1: Server-to-server performance analytics subscription request

Information element	Status	Description
Analytics Consumer ID	M	The identifier of the analytics consumer (VAL server, EES etc.).
Analytics ID	O	The identifier of the analytics event. This ID can be for example “server-to-server performance analytics”.
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions.
List of server identifiers and addresses	M	Identifier of the servers, e.g. SEAL server ID, EASID, EESID, and IP address(es) for which the analytics subscription applies.
VAL service ID	O	The VAL service for which the subscription applies.
Reporting requirements	O	Requirements for analytics reporting. The requirements may include for example the type and frequency of reporting (periodic or event triggered), the reporting periodicity in case of periodic, and reporting thresholds.
Area of Interest	O	The geographical or service area for which the subscription request applies.
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction).
Time validity	O	The time validity of the subscription request.

8.13.3.3 Server-to-server performance analytics subscription response

Table 8.13.3.3-1 describes information elements for the server-to-server performance analytics subscription response from the ADAE server to the analytics consumer.

Table 8.13.3.3-1: Server-to-server performance analytics subscription response

Information element	Status	Description
Result	M	The result of the analytics subscription request (positive or negative acknowledgement).

8.13.3.4 Server-to-server performance analytics notification

Table 8.13.3.4-1 describes information elements for the server-to-server performance analytics notification from the ADAE server to the analytics consumer.

Table 8.13.3.4-1: Server-to-server performance analytics notification

Information element	Status	Description
Analytics ID	O	The identifier of the analytics event. This ID can be for example “server-to-server performance analytics”.
Analytics Output	M	The predictive or statistical parameter, which can be: - A server-to-server session predicted or expected performance change - A server-to-server session performance sustainability over a given time horizon/area - QoS measurements from the session (e.g. latency)
Confidence level	O	For predictive analytics, the achieved confidence level can be provided.

8.13.3.5 Inter-server session data request

Table 8.13.3.5-1 describes information elements for the Inter-server session data request from the target server to the ADAE server.

Table 8.13.3.5-1: Inter-server session data request

Information element	Status	Description
ADAE server ID	M	The identifier of the ADAE server.
Analytics ID	O	The identifier of the analytics event. This ID can be for example “Server-to-server performance analytics”.
Analytics type	M	Whether analytics event is about prediction or statistics.
List of server identifiers and addresses	M	Identifier of the servers, e.g. SEAL server ID, EASID, EESID, and IP address(es) for which the analytics subscription applies.
QoS attributes	M	The QoS attributes (latency, bitrate, jitter, application layer PER) to be collected.
Data collection requirements	O	The requirements for data collection, including the format of data, level of abstraction of data, level of accuracy of data, if the measurements should be from real-time measurements or offline data.
Time validity	O	The time validity of the request.

8.13.3.6 Inter-server session data response

Table 8.13.3.6-1 describes information elements for the Inter-server session data response from the ADAE server to the target server.

Table 8.13.3.6-1: Inter-server session data response

Information element	Status	Description
Results	M	The result of the analytics data request (positive or negative acknowledgement).
Analytics ID	O	The identifier of the analytics event.
List of server identifiers and addresses	O	Identifier of the servers, e.g. SEAL server ID, EASID, EESID, and IP address(es) for which the analytics subscription applies.
Data Output	O	The reported data for the server-to server sessions, which can be in form of offline stats/historical data or real-time measurements on the requested QoS parameters..

8.13.3.7 Server-to-server analytics request

Table 8.13.3.7-1 describes information elements for the server-to-server analytics request from the ADAE server to the A-ADRF.

Table 8.13.3.7-1: Server-to-server analytics request

Information element	Status	Description
ADAE server ID	M	The identifier of the ADAE server.
Analytics ID	M	The identifier of the analytics event.
List of server identifiers and addresses	M	Identifier of the servers, e.g. SEAL server ID, EASID, EESID, for which the analytics subscription applies.
QoS attributes	M	The QoS attributes (latency, bitrate, jitter, application layer PER) to be collected.
Time validity	O	The time validity of the request.

8.13.3.8 Server-to-server analytics response

Table 8.13.3.8-1 describes information elements for the server-to-server analytics response from the A-ADRF to the ADAE server.

Table 8.13.3.8-1: Server-to-server analytics response

Information element	Status	Description
Analytics ID	M	The identifier of the analytics event.
List of server identifiers and addresses	M	Identifier of the servers, e.g. SEAL server ID, EASID, EESID, for which the analytics subscription applies.
Data Output	M	The reported data, which can be in form of measurements or offline/historical data on the requested QoS attributes. The reported data includes historical inter-server performance analytics.

8.14 Procedure for Collision Detection Analytics

8.14.1 General

This clause describes two procedures (covering both subscribe-notify and request-response models in 8.14.2.1 and 8.14.2.2 respectively) for supporting collision detection analytics, where the collision detection analytics are performed based on data collected from the Data Producer (e.g. 5GC NFs (e.g. GMLC, NWDAF), ADAE Client, LM server, LM client, 3rd party LM server) and A-ADRF.

8.14.2 Procedure

8.14.2.1 Subscribe-notify model

Pre-conditions:

- Information about environment, e.g. static devices, are available from the 3rd party LM server.
- The location information about the UEs is available at SEAL LM server and/or LM client.
- The Ranging/Sidelink Positioning information exposure of the UEs is allowed at 5GC.

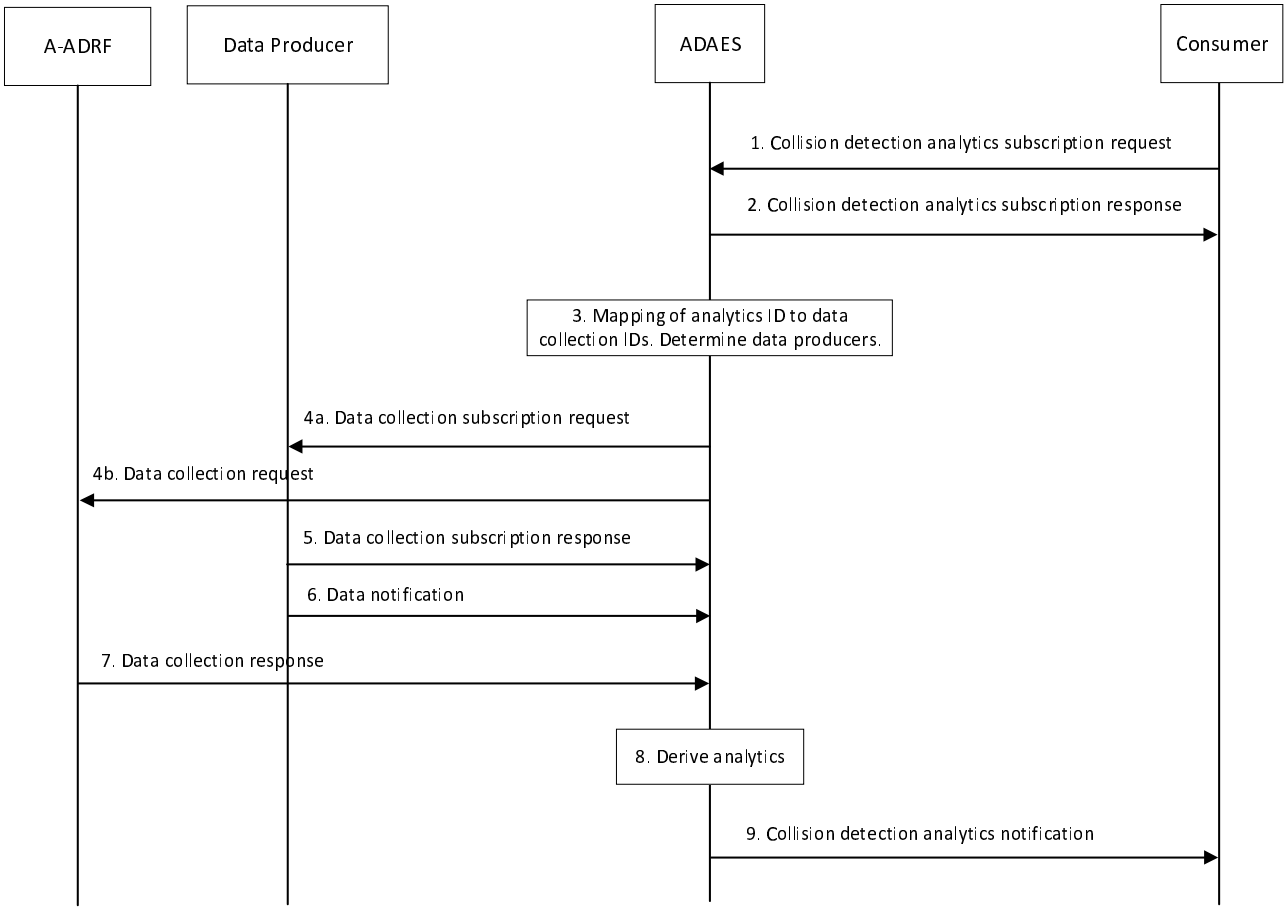

Figure 8.14.2.1-1: ADAES support for collision detection analytics

1. The analytics consumer (e.g. VAL Server, LM server, UAE server, UAS application specific server) sends collision detection analytics subscription request to ADAE server. The Analytics ID in the request message is set to "Collision detection analytics for target UE(s)" or "Collision detection analytics for any UEs". For analytics subscription request, the request contains message as defined in table 8.14.3.2-1.

2. Upon receiving the event subscription request from the consumer, the ADAE server checks for the relevant authorization for the event subscription. If the authorization is successful, the ADAE server stores the request information. The ADAE server sends a service API event subscription response indicating successful subscription.

3. The ADAES maps the analytics event ID to a list of data collection event identifiers, and a list of data producer IDs. Such mapping may be preconfigured by OAM or may be determined by ADAES based on the analytics event type/vertical type and/or data producer profile.

4. The ADAE server sends data collection subscription request to the Data Producer (e.g. 5GC NFs (e.g. GMLC, NWDAF), ADAE Client, LM server, LM client, 3rd party LM server) and a data collection request to the Data Producer (e.g. A-ADRF for historical data) with the respective Data Collection Event ID and the requirement for

collection of ranging and/or sidelink positioning related data or analytics of UEs, and location information of UEs. Data collection at the UE(s) reuses mechanism defined in 3GPP TS 26.531 [3].

5. The Data Producer sends data collection subscription response as a positive or negative acknowledgement to the ADAE server.

6. The ADAE server based on data collection subscription receive ranging and/or sidelink positioning related data/analytics of UEs and location information of UEs from the Data Producer (e.g. 5GC NFs (e.g. GMLC, NWDAF), ADAE Client, LM server, LM client, 3rd party LM server).

NOTE: The procedures for UE related data collection need to take user consent into account.

7. The ADAE server based on data collection request receive ranging and/or sidelink positioning related historical data of UEs from Data Producer (e.g. A-ADRF).

8. The ADAE server performs analytics relevant operations to generate the analytics for the collision detection between any target VAL UEs, collision detection between any UEs and target VAL UEs, or collision detection between any UE within the Area of Interest and based on the request provided in step 1 and the data/analytics received from the Data Producer (e.g. 5GC NFs (e.g. GMLC, NWDAF), ADAE Client, LM server, LM client, 3rd party LM server, A-ADRF for historical data).

9. The ADAE server sends collision detection analytics notifications to the consumer with the required collision detection analytics. The notification contains message as defined in table 8.14.3.4-1.

8.14.2.2 Request-response model

Pre-conditions:

- ADAE Server already have the analytics data derived from steps 3-6 in the procedure introduced in clause 8.14.2.1.

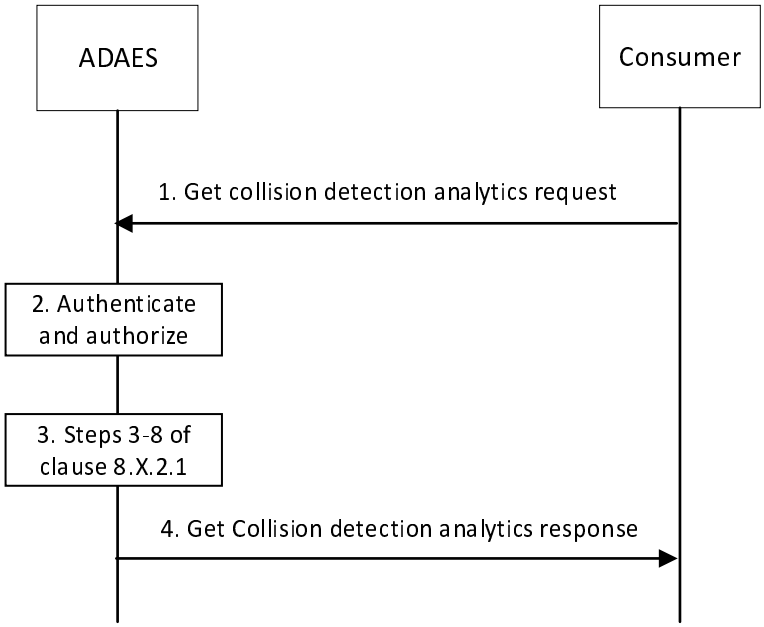

Figure 8.14.2.2-1: ADAES support for collision detection analytics

1. The analytics consumer (e.g. VAL Server, LM Server, UAE server, UAS application specific server) sends a get collision detection analytics request message to the ADAE server to receive analytics data for collision detection analytics with Analytics ID in the request message setting to "Collision detection analytics for target UE(s)" or "Collision detection analytics for any UEs". The request contains message as defined in table 8.14.3.8-1.

2. Upon receiving the request, the ADAE server authenticates and authorizes the analytics consumer.

3. If the analytics consumer is authorized, the ADAE server may get the analytics by performing steps 3 to 8 of clause 8.14.2.1.

4. If the analytics consumer is authorized, the ADAE server sends a get collision detection analytics response message including the analytics data (statistical and/or predictive) of the collision detection analytics as defined in table 8.14.3.9-1.

8.14.3 Information flows

8.14.3.1 General

The following information flows are specified for collision detection analytics based on clause 8.14.2.

8.14.3.2 Collision detection analytics subscription request

Table 8.14.3.2-1 describes the information flow from the consumer (e.g. VAL Server, LM Server, UAE server, UAS application specific server) as a request or update request for the collision detection analytics.

Table 8.14.3.2-1: Collision detection analytics subscription request

Information element	Status	Description
Requestor ID	M (NOTE 1)	The identifier of the consumer.
Analytics ID	O (NOTE 1)	The identifier of the analytics event. This ID can be for example "Collision Detection analytics for target UE(s)", "Collision Detection analytics for any UEs".
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions,
Analytics filter information	M	Filter information for the analytics event.
> Filter for Collision between interested UE(s) and target UE(s)	O (NOTE 2)	The filter information for the Collision Detection analytics for target UE(s).
>>Target VAL UE ID(s)	M	The identifier(s) of VAL UE(s) for which the analytics subscription applies.
>> Interested VAL UE ID(s)	O (see NOTE 3)	The identifier(s) of a list of the interested UE(s) collision with that shall be analysed.
>>Target VAL server ID	O	If consumer is different from the VAL server, this identifier shows the target VAL server for which the analytics subscription applies.
>>Area of Interest	O (see NOTE 3)	The geographical or service area for which the subscription request applies.
> Filter for Collision detection between any UE(s)	O (NOTE 2)	The filter information for the Collision Detection analytics for any UE(s) in an area.
>>Target VAL server ID	O	If consumer is different from the VAL server, this identifier shows the target VAL server for which the analytics subscription applies.
>>Area of Interest	M	The geographical or service area for which the subscription request applies.
Collision detection criteria	O	The parameters for collision detection analytics apply.
>Distance	O	The allowed minimum distance between UEs. The collision is detected if the distance between the UEs is less than the provided value.
Reporting requirements	O	It describes the requirements for analytics reporting. This requirement may include e.g. the type and frequency of reporting (periodic or event triggered), the reporting periodicity in case of periodic, and reporting thresholds in case of event triggered.
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction).
Time validity	O	The time validity of the subscription request.
NOTE 1: This information element shall not be updated. NOTE 2: One of the elements shall be provided. NOTE 3: If the IE "Filter for Collision between the interested UE(s) and target UE(s)" is present, at least one of the elements shall be provided.		

8.14.3.3 Collision detection analytics subscription response

Table 8.14.3.3-1 describes the information elements for the collision detection analytics subscription response from the ADAE server to the consumer.

Table 8.14.3.3-1: Collision detection analytics subscription response

Information element	Status	Description
Result	M	The result of the analytics subscription request (positive or negative acknowledgement).

8.14.3.4 Collision detection analytics notification

Table 8.14.3.4-1 describes the information flow from the ADAES to the consumer (e.g. VAL Server, LM Server, UAE server, UAS application specific server) as a response for the collision detection analytics.

Table 8.14.3.4-1: Collision detection analytics notification

Information element	Status	Description
Analytics ID	M	The identifier of the analytics event. This ID can be for example "Collision Detection analytics for target UE(s)", "Collision Detection analytics for any UEs".
Outputs for Collision between any UE(s) and target UE(s)	O (see NOTE)	The analytics (predictive or statistical parameter) for Collision Detection analytics for target UE(s).
> List of target VAL UE(s)	M	The analytics outputs of the list of target VAL UE(s).
>>Target VAL UE ID	M	The identifier of target VAL UE for which the analytics outputs apply.
>>Potential collision VAL UE ID(s)	M	The identifier(s) of the potential collision VAL UE(s) for which the analytics outputs apply.
>>Time of potential collisions	M	Time of the potential collisions between the target UE and the UEs.
>>Location of potential collisions	M	Location of the potential collisions between the target UE and the UEs.
>>Direction of moving	O	Direction of the target UE and the UEs moving.
>>Velocity of moving	O	Velocity of the target UE and the UEs moving.
>>Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
Outputs for Collision between any UE(s)	O (NOTE)	The analytics (predictive or statistical parameter) for Collision Detection analytics for any UEs.
>Potential collision VAL UE ID(s)	M	The identifier(s) of the potential collision VAL UE(s) for which the analytics outputs apply.
>Time of potential collisions	M	Time of the potential collisions between the UEs.
>Location of potential collisions	M	Location of the potential collisions between the UEs.
>Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
NOTE: One of the elements shall be provided.		

8.14.3.5 Ranging/SL positioning data and location information collection subscription request

Table 8.14.3.5-1 describes information elements for the Ranging/SL positioning data and location information collection subscription request from the ADAE server to the Data Producer, e.g. 5GC NFs (e.g. GMLC, NWDAF), ADAE Client, LM server, LM client, 3rd party LM server, A-ADRF for historical data.

Table 8.14.3.5-1: Data collection subscription request

Information element	Status	Description
Requestor ID	M	The identifier of the consumer.
Data Collection Event ID	M	The identifier of the data collection event
Data Collection requirements	M	The requirements for data collection, including the format of data, frequency of reporting, level of abstraction of data, level of accuracy of data.
Analytics ID	O	The identifier of the analytics event, for which the data collection is needed.
List of Data Producer IDs	O	In case when this request is performed via A-DCCF, then the list of Data Producer IDs is needed.
>Target data producer profile criteria	O	Characteristics of the data producers to be used.
>VAL UE IDs	O	The VAL UE(s) identifiers for which the data/analytics apply.
Area of Interest	O	The geographical or service area for which the requirement request applies.
Time validity	O	The time validity of the request.

8.14.3.6 Ranging/SL positioning data and location information collection subscription response

Table 8.14.3.6-1 describes information elements for the Data collection subscription response from the Data Producer, e.g. 5GC NFs (e.g. GMLC, NWDAF), ADAE Client, LM server, LM client, 3rd party LM server, A-ADRF for historical data.

Table 8.14.3.6-1: Data collection subscription response

Information element	Status	Description
Result	M	The result of the Ranging/SL positioning data and location information collection subscription request (positive or negative acknowledgement).

8.14.3.7 Data Notification

Table 8.14.3.7-1 describes information elements for the Data Notification from the Data Producer to the ADAE server.

Table 8.14.3.7-1: Data notification

Information element	Status	Description
Data Collection Event ID	M	The identifier of the data collection event.
Data Producer ID	M	The identity of Data Producer.
Analytics ID	O	The identifier of the analytics event.
Data Type	M	The type of reported data samples which can be network data, application data, edge data, or different granularities / abstraction of data (e.g. real time, non-real time). This also indicates whether data are offline (from A-ADRF or not).
Data Output	M	The reported data, which can be inform of measurements or offline/historical data on the requested parameter based on subscription. Such data can be ranging/sidelink positioning information of UEs, location information of UEs (moving devices like UAS devices, V2X devices, robots, and/or people with UE), and the location information about environment (static devices like infrastructures) for a given time and area of interest, Relative Proximity analytics.

8.14.3.8 Get analytics data request

Table 8.14.3.8-1 describes information elements for the collision detection analytics request from the analytics consumer to the ADAE server.

Table 8.14.3.8-1: Get analytics data request

Information element	Status	Description
Requestor ID	M	The identifier of the consumer.
Analytics ID	O	The identifier of the analytics event. This ID can be for example "Collision Detection analytics for target UE(s)" , "Collision Detection analytics for any UEs".
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions.
Analytics filter information	M	Filter information for the analytics event
> Filter for Collision between interested UE(s) and target UE(s)	O (see NOTE 1)	The filter information for the Collision Detection analytics for target UE(s).
>>Target VAL UE ID(s)	M	The identifier(s) of VAL UE(s) for which the request applies
>> Interested VAL UE ID(s)	O (see NOTE 2)	The identifier(s) of a list of the interested UE(s) collision with that shall be analysed.
>Target VAL server ID	O	If consumer is different from the VAL server, this identifier shows the target VAL server for which the request applies.
>Area of Interest	O (see NOTE 2)	The geographical or service area for which the subscription request applies
> Filter for Collision detection between any UE(s)	O (see NOTE 1)	The filter information for the Collision Detection analytics for any UE(s) in an area.
>>Target VAL server ID	O	If consumer is different from the VAL server, this identifier shows the target VAL server for which the request applies.
>>Area of Interest	M	The geographical or service area for which the request applies.
Collision detection criteria	O	The parameters for collision detection analytics apply.
>Distance	O	The allowed minimum distance between UEs.
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction).
Time duration	O	Time duration since when analytics data is required.
NOTE 1: One of the elements shall be provided. NOTE 2: If the IE "Filter for Collision between any UE(s) and target UE(s)" is present, at least one of the elements shall be provided.		

8.14.3.9 Get analytics data response

Table 8.14.3.9-1 describes information elements for the Get collision detection analytics response from the ADAE server to the consumer.

Table 8.14.3.9-1: Get analytics response

Information element	Status	Description
Analytics ID	O	The identifier of the analytics event. This ID can be for example "Collision Detection analytics for target UE(s)", "Collision Detection analytics for any UEs"".
Outputs for Collision between any UE(s) and target UE(s)	O (see NOTE)	The analytics (predictive or statistical parameter) for Collision Detection analytics for target UE(s).
> List of target VAL UE(s)	M	The analytics outputs of the list of target VAL UE(s).
>>Target VAL UE ID	M	The identifier of target VAL UE for which the analytics outputs apply.
>>Potential collision VAL UE ID(s)	M	The identifier(s) of the potential collision VAL UE(s) for which the analytics outputs apply.
>>Time of potential collisions	M	Time of the potential collisions between the UEs.
>>Location of potential collisions	M	Location of the potential collisions between the UEs.
>>Direction of moving	O	Direction of the UEs moving.
>>Velocity of moving	O	Velocity of the UEs moving.
>>Timestamp	O	Time stamp of the collected analytics data.
>>Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
Outputs for Collision between any UE(s)	O (see NOTE)	The analytics (predictive or statistical parameter) for Collision Detection analytics for any UEs.
>Potential collision VAL UE ID(s)	M	The identifier(s) of the potential collision VAL UE(s) for which the analytics outputs apply.
>Time of potential collisions	M	Time of the potential collisions between the UEs.
>Location of potential collisions	M	Location of the potential collisions between the UEs.
>Timestamp	O	Time stamp of the collected analytics data.
>Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
NOTE: One of the elements shall be provided.		

8.15 Procedure for Location-related UE Group Analytics

8.15.1 General

This clause describes two procedures (covering both subscribe-notify and request-response models in 8.15.2.1 and 8.15.2.2 respectively) for supporting location-related UE group analytics, where the location-related UE group analytics are performed based on data collected from the Data Producer (e.g. 5GC NFs (e.g. GMLC (via NEF), NWDAF), ADAE Client, LM server) and A-ADRF.

8.15.2 Procedure

8.15.2.1 Subscribe-notify model

Pre-conditions:

- The location information about the UEs is available at SEAL LM server.
- The location information of the UEs exposure is allowed at 5GC.

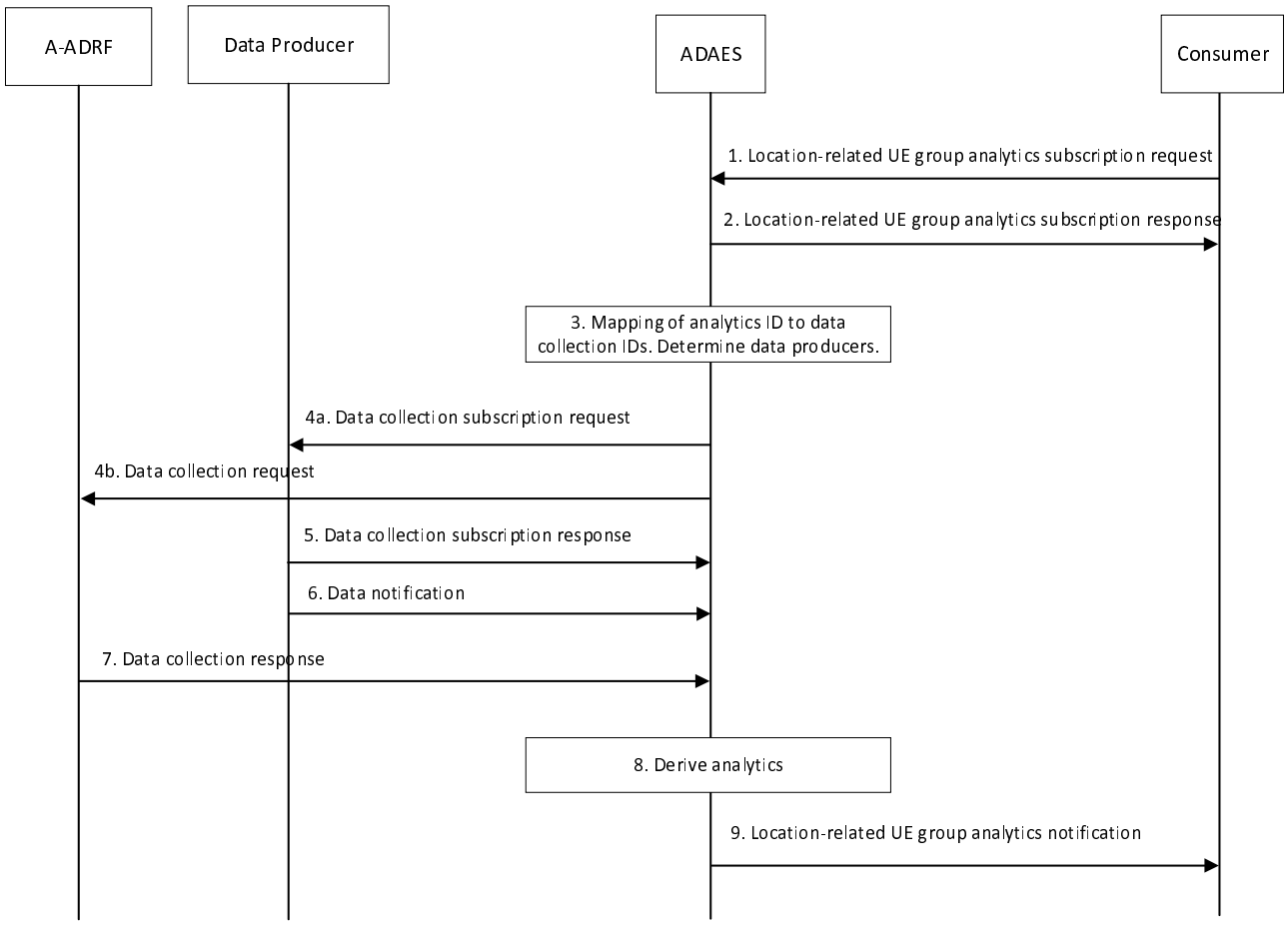

Figure 8.15.2.1-1: ADAES support for location-related UE group analytics

1. The analytics consumer (i.e. LMS) sends location-related UE group analytics subscription request to ADAE server. The Analytics ID in the request message is set to "UE group route analytics" or "UE group member deviation". For analytics subscription request, the request contains message as defined in table 8.15.3.2-1.

2. Upon receiving the event subscription request from the consumer, the ADAE server checks for the relevant authorization for the event subscription. If the authorization is successful, the ADAE server stores the request information. The ADAE server sends a service API event subscription response indicating successful subscription.

3. The ADAES maps the analytics event ID to a list of data collection event identifiers, and a list of data producer IDs. Such mapping may be preconfigured by OAM or may be determined by ADAES based on the analytics event type/vertical type and/or data producer profile.

4. The ADAE server sends a data collection subscription request to the Data Producer (e.g. 5GC NFs (e.g. GMLC (via NEF), NWDAF), ADAE Client, LM server) and a data collection request to the Data Producer (e.g. A-ADRF for historical data) with the respective Data Collection Event ID and the requirement for collection location related data/analytics of UEs. Data collection at the UE(s) reuses the mechanism defined in 3GPP TS 26.531 [3].

5. The Data Producer sends data collection subscription response as a positive or negative acknowledgement to the ADAE server.

6. The ADAE server based on data collection subscription receive location related data/analytics of UEs from the Data Producer (e.g. 5GC NFs (e.g. GMLC (via NEF), NWDAF), ADAE Client, LM server).

7. The ADAE server based on data collection request receive location related historial data of UEs from the Data Producer (e.g. A-ADRF).

NOTE: The procedures for UE location information collection need to take user consent into account.

8. The ADAE server performs analytics relevant operations to generate the analytics based on the data received from the Data Producer (e.g. 5GC NFs (e.g. GMLC, NWDAF), ADAE Client, LM server, A-ADRF for historical data). In detail, the ADAE server may generate analytics in the following ways.

   - For UE group route analytics: Inputs include the location information of UE(s) from LM server (e.g. UE's location in clause 9.3.7 of 3GPP TS 23.434 [2]), the analytics from NWDAF (e.g. UE mobility analytics, Movement behaviour analytics, UE communication analytics, and/or Dispersion analytics in 3GPP TS 23.288 [4]). For example, UE's location service from LMS allows ADAES to obtain the UE location, UE mobility analytics provides potential moving direction of the UE(s), Dispersion analytics gives ADAES information on UE data volume dispersion predictions, etc., by combining all the information collected, predictions on UE group route can be generated.

   - For UE group member deviation analytics: Inputs include the Ranging/Sidelink Positioning location information of the UE group member from GMLC (via NEF) (e.g. Ranging/Sidelink Positioning location results in clause 6.20 of 3GPP TS 23.273 [18]), location information of the UE group member from LM server (e.g. UE's location in clause 9.3.7 of 3GPP TS 23.434 [2]), and the analytics from NWDAF (e.g. UE mobility analytics, Movement behaviour analytics, Relative Proximity analytics, and/or Abnormal behaviour analytics in 3GPP TS 23.288 [4]) of this UE group member. The ADAE server can aggregate the collected information (e.g. distance between UEs from the Ranging/Sidelink Positioning location information service, predictions on distance between UEs from the Relative Proximity analytics, etc.) and derive which UE group member is deviating (or will deviate) from other group member(s) or target group member (e.g. UE's ranging information with any other UE(s) in a group is larger than a threshold, and such trend shows longer and longer ranging within a time period, or the UE moving direction is different from any other UE(s) in a group or target group member).

9. The ADAE server sends location-related UE group analytics notifications to the consumer with the required location-related UE group analytics.

8.15.2.2 Request-response model

Pre-conditions:

- ADAE Server already has the analytics data derived from steps 3-6 in the procedure introduced in clause 8.15.2.1.

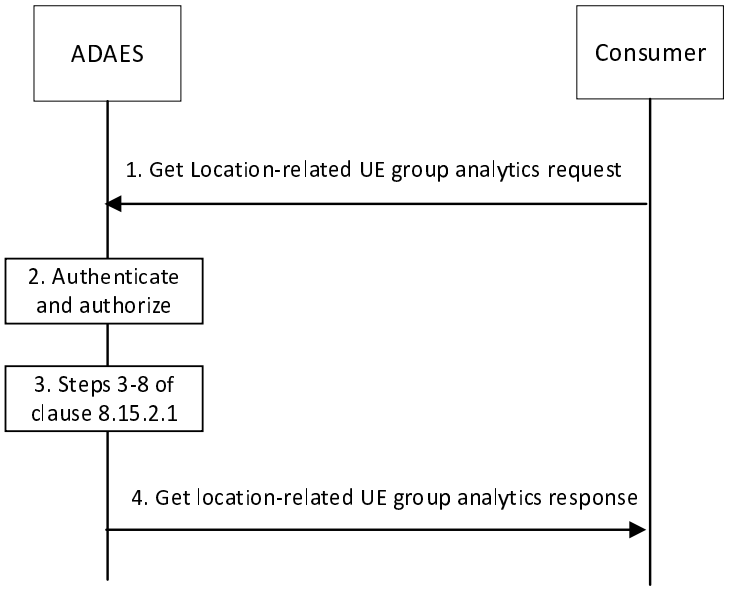

Figure 8.15.2.2-1: ADAES support for location-related UE group analytics

1. The analytics consumer (i.e. LMS) sends a get location-related UE group analytics request message to the ADAE server to receive analytics data for location-related UE group analytics with Analytics ID in the request message setting to "UE group route analytics" or "UE group member deviation". The request contains message as defined in table 8.15.3.8-1.

2. Upon receiving the request, the ADAE server authenticates and authorizes the analytics consumer.
3. If the analytics consumer is authorized, the ADAE server may get the analytics by performing steps 3 to 8 of clause 8.15.2.1.
4. If the analytics consumer is authorized, the ADAE server sends a get location-related UE group analytics response message including the analytics data (statistical and/or predictive) of the location-related UE group analytics.

8.15.3 Information flows

8.15.3.1 General

The following information flows are specified for location-related UE group analytics based on clause 8.15.2.

8.15.3.2 Location-related UE group analytics subscription request

Table 8.15.3.2-1 describes the information flow from the consumer (LMS) as a request or update request for the location-related UE group analytics.

Table 8.15.3.2-1: Location-related UE group analytics subscription request

Information element	Status	Description
Requestor ID	M (NOTE 1)	The identifier of the consumer.
Analytics ID	O (NOTE 1)	The identifier of the analytics event. This ID can be for example "UE group route analytics" or "UE group member deviation analytics".
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions,
Analytics filter information	M	Filter information for the analytics event.
>Application Group ID	O (NOTE 2)	Application group identifier for which the analytics subscription applies.
>Target VAL UE ID(s)	O (NOTE 2)	The identifier(s) of the VAL UE(s) for which the analytics subscription applies.
>Area of Interest	O	The geographical or service area for which the subscription request applies.
>Application Group profile(s)	O	Information about the Application Group(s) with common EAS (as defined in 3GPP TS 23.558 [14] Table 8.15.11-1).
>Deviation	O	Deviation information, e.g. different moving direction or moving speed, distance with the target group member UE larger than an threshold.
>>Target Group member UE ID	O	The identifier of the target group member UE.
>>Deviation criteria	O	The criteria used for detecting deviation of group member UE, e.g. distance, moving direction, moving speed.
Reporting requirements	O	It describes the requirements for analytics reporting. This requirement may include e.g. the type and frequency of reporting (periodic or event triggered), the reporting periodicity in case of periodic, and reporting thresholds.
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction).
Time validity	O	The time validity of the subscription request.
NOTE 1: This information element shall not be updated. NOTE 2: One of the elements shall be provided.		

8.15.3.3 Location-related UE group analytics subscription response

Table 8.15.3.3-1 describes the information elements for the location-related UE group analytics subscription response from the ADAE server to the consumer.

Table 8.15.3.3-1: Location-related UE group analytics subscription response

Information element	Status	Description
Result	M	The result of the analytics subscription request (positive or negative acknowledgement).

8.15.3.4 Location-related UE group analytics notification

Table 8.15.3.4-1 describes the information flow from the ADAES to the consumer (LM Server) as a response for the location-related UE group analytics.

Table 8.15.3.4-1: Location-related UE group analytics notification

Information element	Status	Description
Analytics ID	M	The identifier of the analytics event. This ID can be for example "UE group route analytics" or "UE group member deviation analytics".
Outputs for UE group route	O (NOTE 1)	The reported analytics for UE group route analytics apply.
>List of EAS ID(s)	M	List of identifiers of EAS.
>>EAS ID(s)	O	Identifier(s) of EAS(s).
>>Route ID	M	The identifier of the common route for the UE(s) to EAS(s).
>>VAL UE ID(s)	M	The identifiers of the VAL UE(s) which with the common route to the EAS(s).
Outputs for UE group member deviation	O (NOTE 1, NOTE 2)	The reported analytics for group member deviation analytics apply.
>Application Group ID	M	Application group identifier.
>>Target Group member UE ID	O	The identifier of the target group member UE.
>List of VAL UE ID(s)	M	The VAL UE(s) which with different behaviour with the majority group members or the target group member.
>>VAL UE ID	O	Identifier of the VAL UE.
>>Deviation	O	Detail information of deviation for the VAL UE, e.g., different moving direction or moving speed, distance with the target group member.
>>Time duration	O	The time duration of this UE deviation.
Validity Time	O	The valid time duration of the analytics.
Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
NOTE 1: One of these shall be present based on the analytics event. NOTE 2: Statistics on UE deviation including e.g. minimum, maximum, and average UEs moving into area, moving out of area, moving speed, and distance from target group member.		

8.15.3.5 Location information collection subscription request

Table 8.15.3.5-1 describes information elements for the Ranging/SL positioning data and location information collection subscription request from the ADAE server to the Data Producer, e.g. 5GC NFs (e.g. GMLC, NWDAF), ADAE Client, LM server, A-ADRF for historical data.

Table 8.15.3.5-1: Data collection subscription request

Information element	Status	Description
Requestor ID	M	The identifier of the consumer.
Data Collection Event ID	M	The identifier of the data collection event
Data Collection requirements	M	The requirements for data collection, including the format of data, frequency of reporting, level of abstraction of data, level of accuracy of data.
Analytics ID	O	The identifier of the analytics event, for which the data collection is needed. This ID can be for example "UE group route analytics" or "UE group member deviation analytics".
List of Data Producer IDs	O	In case when this request is performed via A-DCCF, then the list of Data Producer IDs is needed.
>Target data producer profile criteria	O	Characteristics of the data producers to be used.
>VAL UE IDs	O	The VAL UE(s) identifiers for which the data/analytics apply.
Area of Interest	O	The geographical or service area for which the requirement request applies.
Time validity	O	The time validity of the request.

8.15.3.6 Location information collection subscription response

Table 8.15.3.6-1 describes information elements for the Data collection subscription response from the Data Producer, e.g. 5GC NFs (e.g. GMLC, NWDAF), ADAE Client, LM server, A-ADRF for historical data.

Table 8.15.3.6-1: Data collection subscription response

Information element	Status	Description
Result	M	The result of the location information collection subscription request (positive or negative acknowledgement).

8.15.3.7 Data Notification

Table 8.15.3.7-1 describes information elements for the Data Notification from the Data Producer to the ADAE server.

Table 8.15.3.7-1: Data notification

Information element	Status	Description
Data Collection Event ID	M	The identifier of the data collection event.
Data Producer ID	M	The identity of Data Producer.
Analytics ID	O	The identifier of the analytics event. This ID can be for example "UE group route analytics" or "UE group member deviation analytics".
Data Type	M	The type of reported data samples which can be network data, application data, edge data, or different granularities / abstraction of data (e.g. real time, non-real time). This also indicates whether data are offline (from A-ADRF or not).
Data Output	M	The reported data, which can be inform of measurements or offline/historical data on the requested parameter based on subscription. Such data can be location information of UEs (moving devices like UAS devices, V2X devices, robots, and/or people with UE, static devices like infrastructures) for a given time and area of interest, measurement of UE(s) moving in or moving out of the area of interest, UE mobility analytics, Ranging/Sidelink Positioning location information of UEs, Movement behaviour analytics, UE communication analytics, Dispersion analytics, Relative Proximity analytics, and/or Abnormal behaviour analytics.

8.15.3.8 Get analytics data request

Table 8.15.3.8-1 describes information elements for the location-related UE group analytics request from the analytics consumer to the ADAE server.

Table 8.15.3.8-1: Get analytics data request

Information element	Status	Description
Requestor ID	M	The identifier of the consumer.
Analytics ID	M	The identifier of the analytics event. This ID can be for example "UE group route analytics" or "UE group member deviation analytics".
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions,
Analytics filter information	M	Filter information for the analytics event.
>Application Group ID	O (NOTE)	Application group identifier for which the analytics subscription applies.
>Target VAL UE ID(s)	O (NOTE)	The identifier(s) of the VAL UE(s) for which the analytics subscription applies.
>Area of Interest	O	The geographical or service area for which the subscription request applies.
>Application Group profile(s)	O	Information about the Application Group(s) with common EAS (as defined in 3GPP TS 23.558 [14] Table 8.15.11-1).
>Deviation	O	Deviation information, e.g. different moving direction or moving speed, distance with the target group member UE larger than a threshold.
>>Target Group member UE ID	O	The identifier of the target group member UE.
>>Deviation criteria	O	The criteria used for detecting deviation of group member UE, e.g. distance, moving direction, moving speed.
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction).
NOTE: One of elements shall be provided.		

8.15.3.9 Get analytics data response

Table 8.15.3.9-1 describes information elements for the Get location-related UE group analytics response from the ADAE server to the consumer.

Table 8.15.3.9-1: Get analytics response

Information element	Status	Description
Analytics ID	M	The identifier of the analytics event. This ID can be for example "UE group route analytics" or "UE group member deviation analytics".
Outputs for UE group route	O (NOTE 1)	The reported analytics for UE group route analytics apply.
>List of EAS ID(s)	M	List of identifiers of EAS.
>>EAS ID(s)	O	Identifier(s) of EAS(s).
>>Route ID	M	The identifier of the common route for the UE(s) to EAS(s).
>>VAL UE ID(s)	M	The identifiers of the VAL UE(s) which with the common route to the EAS(s).
>Timestamp	O	Time stamp of the collected analytics data.
Outputs for UE group member deviation	O (NOTE 1, NOTE 2)	The reported analytics for group member deviation analytics apply.
>Application Group ID	M	Application group identifier.
>>Target Group member UE ID	O	The identifier of the target group member UE.
>List of VAL UE ID(s)	M	The VAL UE(s) which with different behaviour with the majority group members or the target group member.
>>VAL UE ID	O	Identifier of the VAL UE.
>>Deviation	O	Detail information of deviation for the VAL UE, e.g., different moving direction or moving speed, distance with the target group member.
>>Time duration	O	The time duration of this UE deviation.
>Timestamp	O	Time stamp of the collected analytics data.
Validity Time	O	The valid time duration of the analytics.
Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
NOTE 1: One of these shall be present based on the analytics event. NOTE 2: Statistics on UE deviation including e.g. minimum, maximum, and average UEs moving into area, moving out of area, moving speed, and distance from target group member.		

8.16 Procedure for Application Layer AI/ML Member Capability Analytics

8.16.1 General

This clause describes two procedures (covering both subscribe-notify and request-response models in 8.16.2.1 and 8.16.2.2 respectively) for supporting application layer AI/ML member capability analytics, where the application layer AI/ML member capability analytics are performed based on data collected from the Data Producer (e.g. ADAE client) and A-ADRF.

8.16.2 Procedure

8.16.2.1 Subscribe-notify model

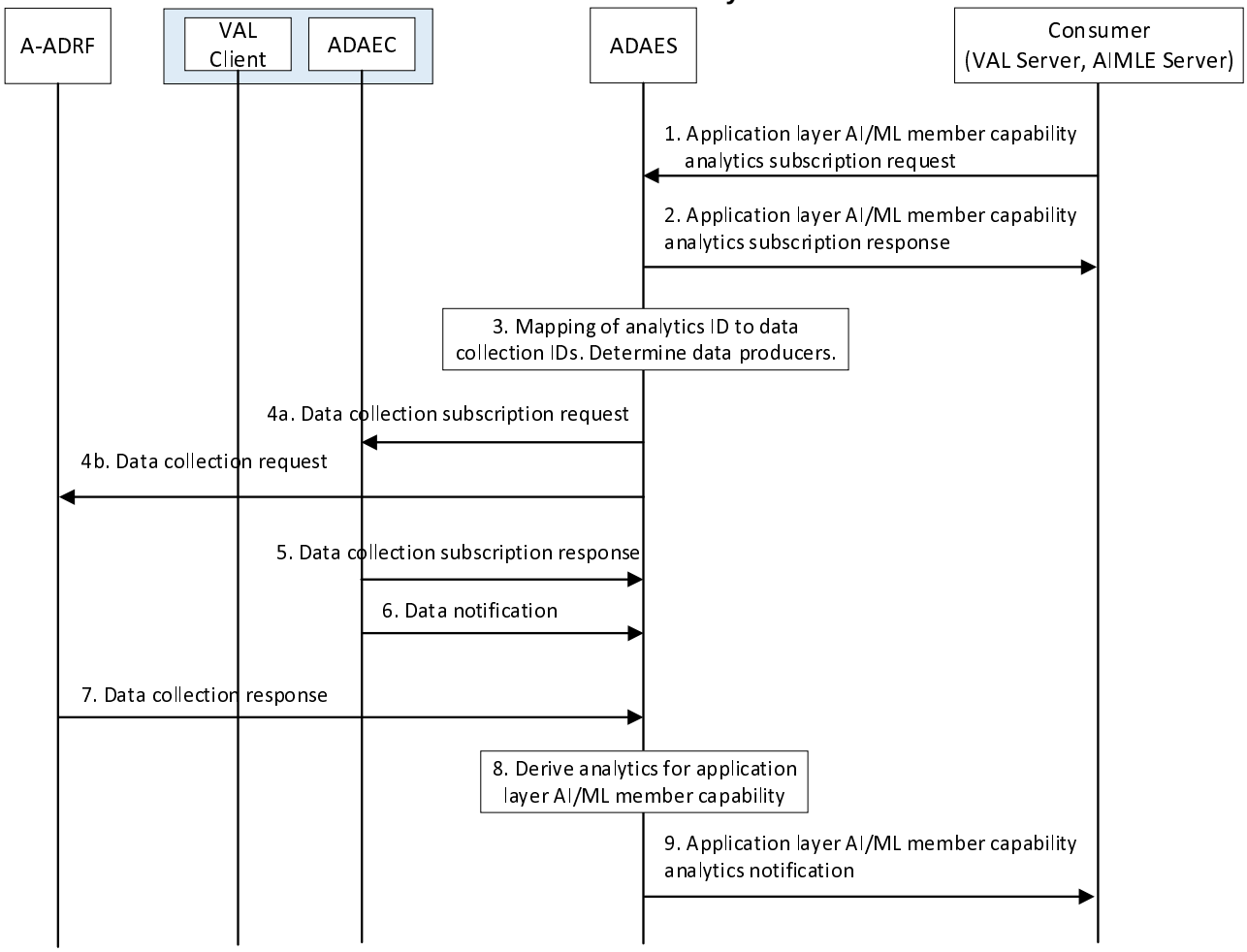

Figure 8.16.2.1-1: ADAES support for application layer AI/ML Member capability analytics

1. The analytics consumer (e.g. VAL Server, AIMLE Server) sends application layer AI/ML member capability analytics subscription request to ADAE server. For analytics subscription request, the request contains message as defined in Table 8.16.3.2-1.

2. Upon receiving the event subscription request from the consumer, the ADAE server checks for the relevant authorization for the event subscription. If the authorization is successful, the ADAE server stores the request information. The ADAE server sends a service API event subscription response indicating successful subscription.

3. The ADAES maps the analytics event ID to a list of data collection event identifiers, and a list of data producer IDs. Such mapping may be preconfigured by OAM or may be determined by ADAES based on the analytics event type/vertical type and/or data producer profile.

4. The ADAE server sends a data collection subscription request to the Data Producers (ADAE client) or a data collection request to the Data Producers (A-ADRF) with the respective Data Collection Event ID and the requirement for data collection. Data collection at the UE(s) reuses the mechanism defined in 3GPP TS 26.531 [3].

5. The Data Producers (ADAE client) send data collection subscription response as a positive or negative acknowledgement to the ADAE server.

6. The ADAE server based on data collection subscription receive data on the application layer AI/ML Member capability based on the data collection event ID from ADAE client.

7. The ADAE server based on data collection request receive data/analytics on the application layer AI/ML Member capability based on the data/analytics collection event ID from A-ADRF.

NOTE 1: The procedures for data collection for application layer AI/ML Member capability analytics need to take user consent into account.

8. The ADAES performs analytics relevant operations to generate the analytics based on the data/analytics received from the ADAEC.

9. The ADAES sends application layer AI/ML member capability analytics notifications to the consumer with the required application layer AI/ML Member capability analytics.

NOTE 2: The format for the application layer AI/ML Member capability attributes will be standardized in stage 3.

8.16.2.2 Request-response model

Pre-conditions:

- ADAE server already have the analytics data derived from steps 3-8 in the procedure introduced in clause 8.16.2.1.

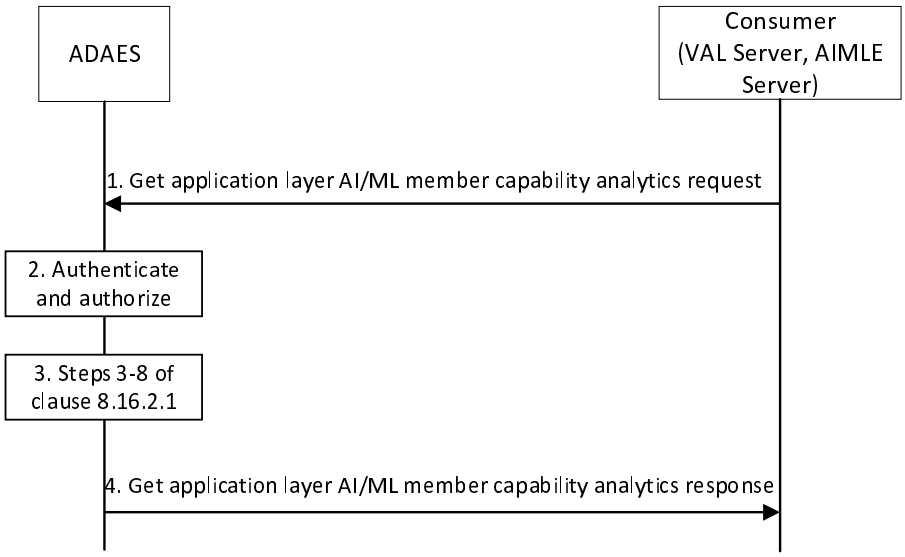

Figure 8.16.2.2-1: ADAES support for application layer AI/ML Member capability analytics

1. The analytics consumer (e.g. VAL Server, AIMLE Server) sends a get application layer AI/ML member capability analytics request message to the ADAE server to receive analytics data for application layer AI/ML Member capability. The request contains message as defined in Table 8.16.3.8-1.

2. Upon receiving the request, the ADAE server authenticates and authorizes the analytics consumer.

3. If the analytics consumer is authorized, the ADAE server may get the analytics by performing step 3 to 8 of clause 8.16.2.1.

4. The ADAE server sends a get application layer AI/ML member capability analytics response message including the analytics data (statistical and/or predictive) of the application layer AI/ML Member capability.

8.16.3 Information flows

8.16.3.1 General

The following information flows are specified for application layer AI/ML Member capability analytics based on clause 8.16.2.

8.16.3.2 Application Layer AI/ML Member capability analytics subscription request

Table 8.16.3.2-1 describes the information flow from the consumer (e.g. VAL server, AIMLE server) as a request or update request for the application layer AI/ML Member capability analytics.

Table 8.16.3.2-1: Application Layer AI/ML Member capability analytics subscription request

Information element	Status	Description
Requestor ID	M (NOTE)	The identifier of the consumer.
Analytics ID	M (NOTE)	The identifier of the analytics event. This ID can be for example "Application layer AI/ML Member capability analytics".
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions.
List of VAL users or AI/ML Member IDs	M	The VAL users or AI/ML Member (s) identifiers for which the data/analytics apply.
VAL service ID	O	The identifier of the VAL service which is associated with application layer AI/ML Member capability.
Application layer AI/ML Member capability attributes	M	The application layer AI/ML Member capability attributes to be analyzed at the ADAE client, e.g. communication capability (e.g. maximum/minimum number of supported active connections).
Reporting requirements	O	It describes the requirements for analytics reporting. This requirement may include e.g. the type and frequency of reporting (periodic or event triggered), the reporting periodicity in case of periodic, and reporting thresholds.
Area of Interest	O	The geographical or service area for which the subscription request applies.
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction).
Time validity	O	The time validity of the subscription request.
NOTE: This information element shall not be updated.		

8.16.3.3 Application Layer AI/ML Member capability analytics subscription response

Table 8.16.3.3-1 describes the information elements for the application layer AI/ML Member capability analytics subscription response from the ADAE server to the consumer.

Table 8.16.3.3-1: Application layer AI/ML Member capability analytics subscription response

Information element	Status	Description
Result	M	The result of the analytics subscription request (positive or negative acknowledgement).

8.16.3.4 Application layer AI/ML Member capability analytics notification

Table 8.16.3.4-1 describes the information flow from the ADAES to the consumer (e.g. VAL Server, AIMLE Server) as a response for the application layer AI/ML Member capability analytics.

Table 8.16.3.4-1: Application layer AI/ML Member capability analytics notification

Information element	Status	Description
Analytics ID	M	The identifier of the analytics event. This ID can be for example "Application layer AI/ML Member capability analytics".
List of VAL users or AI/ML Member IDs	M	The VAL users or AI/ML Member(s) identifiers for which the data/analytics apply.
>VAL user or AI/ML Member ID in the list	M	The VAL user or AI/ML Member identifier for which the data/analytics apply.
>>Analytics Output	M	The analytics outputs for the application layer AI/ML Member capability, which can be the predictive or statistical parameter.
>>>Applicable time period	O	The time period that the analytics applies to.
>>>AI/ML member availability	M	Statistics or predictions of the availability of the AI/ML member, e.g. if the AI/ML member will be up or down during the applicable time period.
>>>AI/ML member capability	M	Statistics or predictions of the capability of the AI/ML member, e.g. maximum/minimum number of supported active connections.
>>Confidence level	O	For predictive analytics, the achieved confidence level can be provided.

8.16.3.5 Application Layer AI/ML Member capability data collection subscription request

Table 8.16.3.5-1 describes information elements for the application layer AI/ML Member capability data collection subscription request from the ADAE server to the Data Producer at the ADAE client or the A-ADRF.

Table 8.16.3.5-1: Data collection subscription request

Information element	Status	Description
Requestor ID	M	The identifier of the consumer.
Data Collection Event ID	M	The identifier of the data collection event
Data collection requirements	O	The requirements for data collection, including the format of data, frequency of reporting, level of abstraction of data, level of accuracy of data.
Analytics ID	O	The identifier of the analytics event, for which the data collection is needed. This ID can be for example "Application layer AI/ML Member capability analytics".
List of Data Producer IDs	O	In case when this request is performed via A-DCCF, then the list of Data Producer IDs is needed.
Target data producer profile criteria	O	Characteristics of the data producers to be used.
List of VAL users or AI/ML Member IDs	M	The VAL users or AI/ML Member (s) identifiers for which the data/analytics apply.
VAL service ID list	O	The identifier(s) of the VAL service(s) which is associated with application layer AI/ML Member capability.
Application layer AI/ML Member capability attributes	M	The application layer AI/ML Member capability attributes to be analyzed at the ADAE client.
Area of Interest	O	The geographical or service area for which the requirement request applies.
Time validity	O	The time validity of the request.

8.16.3.6 Application Layer AI/ML Member capability data collection subscription response

Table 8.16.3.6-1 describes information elements for the Data collection subscription response from the application layer AI/ML Member capability data Producer at the ADAE client or the A-DCCF to the ADAE server.

Table 8.16.3.6-1: Data collection subscription response

Information element	Status	Description
Result	M	The result of the application layer AI/ML Member capability data collection subscription request (positive or negative acknowledgement).

8.16.3.7 Data Notification

Table 8.16.3.7-1 describes information elements for the Data Notification from the Data Producer to the ADAE server.

Table 8.16.3.7-1: Data notification

Information element	Status	Description
Data Collection Event ID	M	The identifier of the data collection event.
Data Producer ID	M	The identity of Data Producer.
Analytics ID	O	The identifier of the analytics event. This ID can be for example "Application layer AI/ML Member capability analytics".
Data Type	M	The type of reported data samples which can be network data, application data, edge data, or different granularities / abstraction of data (e.g. real time, non-real time). This also indicates whether data are offline (from A-ADRF or not).
Data Output	M	The reported data, which can be inform of measurements or offline/historical data on the requested parameter based on subscription.

8.16.3.8 Get analytics data request

Table 8.16.3.8-1 describes information elements for the Get application layer AI/ML Member capability analytics request from the analytics consumer to the ADAE server.

Table 8.16.3.8-1: Get analytics data request

Information element	Status	Description
Requestor ID	M	The identifier of the consumer.
Analytics ID	M	The identifier of the analytics event. The identifier of the analytics event. This ID can be for example "Application layer AI/ML Member capability analytics".
Analytics type	M	The type of analytics, e.g. statistics or predictions.
List of VAL users or AI/ML Member IDs	M	The VAL users or AI/ML Member (s) identifiers for which the data/analytics apply.
VAL service ID	O	The identifier of the VAL service which is associated with application layer AI/ML Member capability.
Application layer AI/ML Member capability attributes	M	The application layer AI/ML Member capability attributes to be analyzed at the ADAE client, e.g. communication capability (e.g. maximum/minimum number of supported active connections).
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction).
Time window	O	The start and end time requirements on the generation of the analytics data to be collected.
Time validity	O	The time validity of the request.

8.16.3.9 Get analytics data response

Table 8.16.3.9-1 describes information elements for the Get application layer AI/ML Member capability analytics response from the ADAE server to the consumer.

Table 8.16.3.9-1: Get analytics response

Information element	Status	Description
Result	M	The result of the analytics data request (positive or negative acknowledgement).
Analytics ID	O	The identifier of the analytics event. This ID can be for example "Application layer AI/ML Member capability analytics".
List of VAL users or AI/ML Member IDs	M	The VAL users or AI/ML Member(s) identifiers for which the data/analytics apply.
>VAL user or AI/ML Member ID in the list	M	The VAL user or AI/ML Member identifier for which the data/analytics apply.
>>Analytics Output	M	The analytics outputs, which can be predictive or statistical parameter.
>>>AI/ML member availability	M	Statistics or predictions of the availability of the AI/ML member, e.g. if the AI/ML member will be up or down during the applicable time period.
>>>AI/ML member capability	M	Statistics or predictions of the capability of the AI/ML member, e.g. maximum/minimum number of supported active connections.
>>Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
>>Timestamp	O	Timestamp of the analytics output.

8.17 Procedure VAL performance analytics for tethered UEs

8.17.1 General

The clause provides a mechanism for analyzing the delay for application layer segments withinan end-to-end XR application service segment, and in particular the link between the VAL Client (e.g., SEALDD client) at the Tethered Device, and the 3GPP VAL UE. Based on this analysis, the mechanism includes the derivation of application layer statistics or predictions for the segment of interest towards the consumer.

8.17.2 Procedure

The procedure associated with the ADAE analytics for tethered UE and application connectivity performance is described below as depicted in Figure 8.17.2-1.

Pre-conditions:

1. A connection between an ADAEC and ADAES is established.
2. A connection between tethered VAL UE and host VAL UE is established.

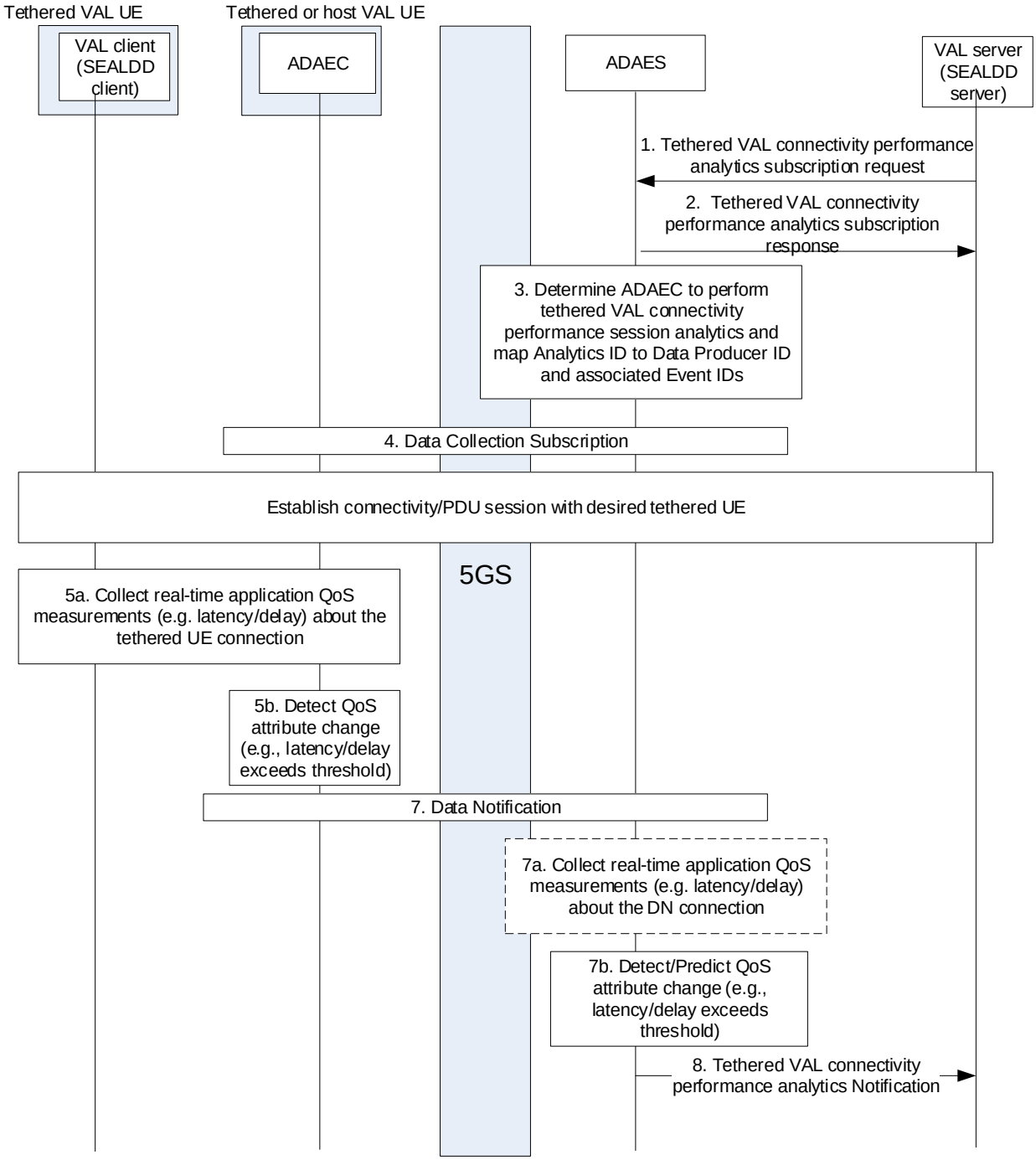

Figure 8.17.2-1: Tethered VAL connectivity performance analytics procedure

1. The consumer of the ADAES analytics service, e.g., the SEALDD server or VAL server, sends a subscription request to ADAES and provides the analytics event ID e.g., "tethered VAL connectivity performance".

2. The ADAES sends a subscription response as an ACK to the consumer.

3. The ADAES maps the analytics ID (i.e., tethered VAL UE connectivity performance) to a list of data collection event identifiers, and optionally a list of data producer IDs. Such mapping may be preconfigured by the ADAES itself based on ASP preferred event types, or VAL type, or alternatively may be preconfigured by an MNO by means of the OAM.

4. The ADAES sends a tethered VAL UE connectivity performance data request to the determined tethered ADAEC with the analytics event ID and the configuration of the reporting required (e.g., periodic, based on maximum delay threshold etc.). Such request also includes additional application QoS attributes to be analyzed additionally based on other metrics (tethered link delay, E2E delay, 5GS PER, 5GS PDB/PSDB etc.). This step

reuses the data collection subscription request and data collection subscription response flows as in clauses 8.2.4.4 and 8.2.4.5 respectively.

An application session then starts between the tethered VAL UE and the VAL server.

The next steps may happen asynchronously and in parallel given the 5GC reporting of events for the configured data collection.

5a. The ADAEC starts collecting data from the tethered VAL UE based on the request. The collection and reporting can be similar to ADAE procedure on VAL session performance analytics (as in step 8 of clause 8.2.3 in 3GPP TS 23.436). As enhancement of existing data collection, ADAEC may collect various events related to tethered link delay, e.g., *TetheredLinkDelayExperience*. This data can thus be about the delay measurements, throughput (e.g., max WiFi capacity), QoE measurements, etc.

5b. The ADAEC detects/predicts an application QoS change. Such a change can be for example a change in the QoS attributes requirements by means of detecting an event where the maximum latency threshold (e.g., over the tethered link or end to end) accepted by the ASP is exceeded, whereas the detection mechanism is performed over a given time horizon based on the analytics subscription request.

6. The ADAES sends a tethered VAL UE connectivity performance data response to the ADAES, including the detected/predicted application QoS change. This step reuses the Data Notification message as in clause 8.2.4.6.

7a. The ADAES may optionally further collect data about the DN performance analytics by means of NWDAF events consumption including service experience analytics etc. This type of analytics will provide statistics/predictions on the user plane performance over a specific application server instance and can be used to predict possible service experience downgrade/deviation that could be used as input to step 7b to predict an application QoS change.

7b. The ADAES predicts an application QoS change. Such a change can be for example a change in the QoS attributes requirements by means of predicting (based on collected metrics and detection in step 5b) an event where the maximum latency threshold (e.g., over the tethered link, over the DN link, or over the E2E connectivity) accepted by the ASP is likely to be exceeded over a given time horizon based on the analytics subscription request.

NOTE: How the DN performance analytics together with the ADAEC measurements are used together to trigger an event related to application QoS change is up to implementation.

8. The ADAES sends the derived analytics notification to the consumer (e.g., VAL server or any other authorized AF consumer).

8.17.3 Information flows

8.17.3.1 General

The following information flows are specified for tethered VAL connectivity performance analytics based on 8.17.2.

8.17.3.2 Tethered VAL connectivity performance analytics subscription request

Table 8.17.3.2-1 describes information elements for the tethered VAL connectivity performance analytics subscription request from the VAL server / Consumer to the ADAE server.

Table 8.17.3.2-1: Tethered VAL connectivity performance analytics subscription request

Information element	Status	Description
Consumer ID	M	The identifier of the analytics consumer
Analytics ID	M	The identifier of the analytics event. This ID can be for example “tethered VAL connectivity performance analytics”.
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions.
VAL service ID	M	The identifier of the VAL service for which analytics subscription apply.
Target tethered VAL UE ID(s)	O	The tethered VAL UE(s) for which the analytics subscription applies.
Target VAL server ID	O	If consumer is different from the VAL server, this identifier shows the target VAL server for which the analytics subscription applies.
Target data producer profile criteria	O	Characteristics of the data producers to be used.
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction.
Area of Interest	O	The geographical or service area for which the subscription request applies.
Time validity	O	The time validity of the subscription request
Reporting requirements	O	It describes the requirements for analytics reporting. This requirement may include e.g. the type and frequency of reporting (periodic or event triggered), the reporting periodicity in case of periodic, and reporting thresholds.

8.17.3.3 Tethered VAL connectivity performance analytics subscription response

Table 8.17.3.3-1 describes information elements for the Tethered VAL connectivity performance analytics subscription response from the ADAE server to the consumer/VAL server.

Table 8.17.3.3-1: VAL performance analytics subscription response

Information element	Status	Description
Result	M	The result of the analytics subscription request (positive or negative acknowledgement).

8.18 Procedure for supporting DN Energy Efficiency analytics

8.18.1 General

This clause describes the procedure for DN energy consumption/efficiency analytics, where the analytics are performed based on data collected from one or more DNs and A-ADRF.

8.18.2 Procedure

Figure 8.18.2-1 illustrates the procedure for DN energy efficiency analytics enablement solution.

Pre-conditions:

1. Data producers (e.g. A-ADRF, EAS, EES) may be pre-configured with data producer profiles (as in Table 8.2.4.8-1) for the data they can provide. ADAES has discovered available data producers and their data producer profiles.

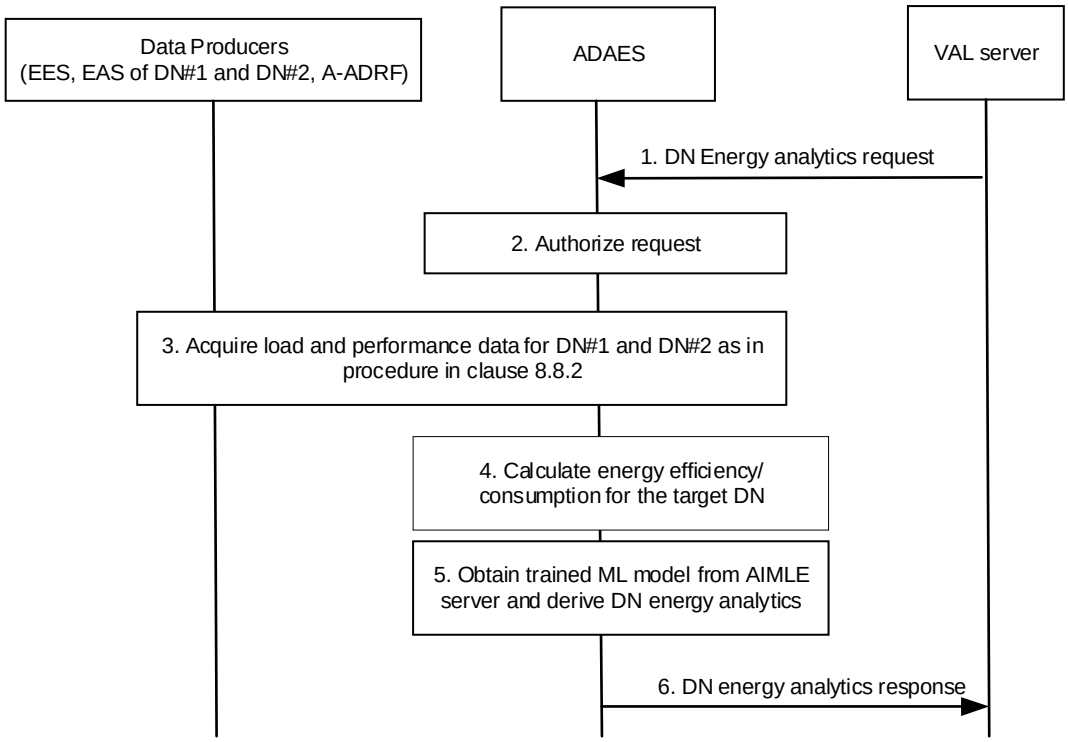

Figure 8.8.2.1-1: ADAES support for DN energy analytics

1. The VAL server sends a DN energy analytics request to ADAES to perform analytics on the DN Energy Consumption/Efficiency for one or more DNs/EDNs, Event ID= “DN energy analytics”, for a given DN service area (or subarea) and a given time window.

2. The ADAES authorizes the VAL request.

3. The ADAES requests and receives from the EAS /VAL servers hosted at the serving and target DNs (within the VAL service area), expected application service load and traffic schedules for the ongoing or future sessions within the area. Such data include traffic schedule report for the VAL Server, and this step re-uses the step 3 to 10 of clause 8.8.2.1.

4. The ADAES calculates the expected energy consumption or efficiency based on the received traffic and load data for the given DNN/DNAI based on the request.

NOTE: How the collected data are used to calculate energy efficiency metric is up to implementation.

5. The ADAES obtains the corresponding trained ML model based on procedure in 3GPP TS 23.482 clause 8.3.2 and performs analytics to derive the predicted energy consumption at the target area and time horizon. The analytics outputs can be the predicted energy consumption / efficiency for the given DNN/DNAI.

6. The ADAES sends a DN energy analytics response with the energy consumption/efficiency analytics output data to the VAL server.

Based on 6, the VAL server can use these analytics as input to trigger pro-actively:

- an application server migration to a different edge cloud or to a centralized cloud as a way of reducing the energy consumption for the edge (if consumption is expected to be very high (e.g. higher than a pre-configured threshold)).

- an application server offboarding and the instantiation of a new server at the target edge/centralized cloud to minimize energy consumption of the edge platform (taking into account the system wide energy efficiency).

8.18.3 Information flows

8.18.3.1 General

The following information flows are specified for DN energy analytics based on clause 8.18.2.

8.18.3.2 DN energy analytics request

Table 8.18.3.2-1 describes information elements for the DN energy analytics request from the VAL server to the ADAE server.

Table 8.8.3.2-1: DN energy analytics request

Information element	Status	Description
Analytics Consumer ID	M	The identifier of the analytics consumer (VAL server, EAS).
Analytics ID	M	The identifier of the analytics event. This ID can be for example “edge performance analytics”.
Analytics type	M	The type of analytics for the event, e.g. statistics or predictions.
DNN/DNAI	M	DNN or DNAIs information for which the subscription applies.
Energy Efficiency/Consumption metrics	O	The formula and necessary metrics for calculating the EE based on load and traffic information per DN.
Target data producer profile criteria	O	Characteristics of the data producers to be used.
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction).
Area of Interest	O	The geographical or service area for which the subscription request applies.
Time validity	O	The time validity of the subscription request.
Reporting requirements	O	It describes the requirements for the energy analytics reporting. This requirement may include e.g. the type and frequency of reporting (periodic or event triggered), the reporting periodicity in case of periodic, and reporting thresholds.

8.18.3.3 DN energy analytics response

Table 8.18.3.3-1 describes information elements for the DN energy analytics request from the VAL server to the ADAE server.

Table 8.18.3.3-1: DN energy analytics response

Information element	Status	Description
Result	M	The result of the analytics request (positive or negative acknowledgement).
Analytics ID	O	The identifier of the analytics event.
Analytics Output	O	The predictive or statistical parameter, which can be stats or prediction related to the energy consumption or efficiency for the edge platform for a given area/time and based on the event type.
> DNN	M	Identifies the data network name for which analytics information is provided.
> DNAI	M	Identifier of a user plane access to one or more DN(s) of the DN.
> Energy metrics	O	The predicted energy metrics.
>> Energy Consumption (NOTE)	O	The predicted energy consumption per DNAI based on network and edge resource usage
>> Energy Efficiency (NOTE)	O	The energy efficiency per DNAI based on network and edge resource usage (given a certain optimal energy consumption metric, which can be pre-configured).
>> DN Data Volume (NOTE)	O	The predicted data volume per DNAI.
> Area of Interest	O	The area (topological or geographical or edge area) where the analytics apply.
> Applicable time period	O	The time period that the analytics applies to.
>Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
NOTE: At least one of these shall be present.		

8.19 Procedure for ML Model Performance Degradation Detection

8.19.1 General

This clause describes a procedure for ML model performance degradation detection for supporting application layer AI/ML operations.

8.19.2 Procedure

Pre-conditions:

- An ADAE Server, acting as an AIMLE consumer, receives a trained ML model (or ML model information) from the AIMLE Server.

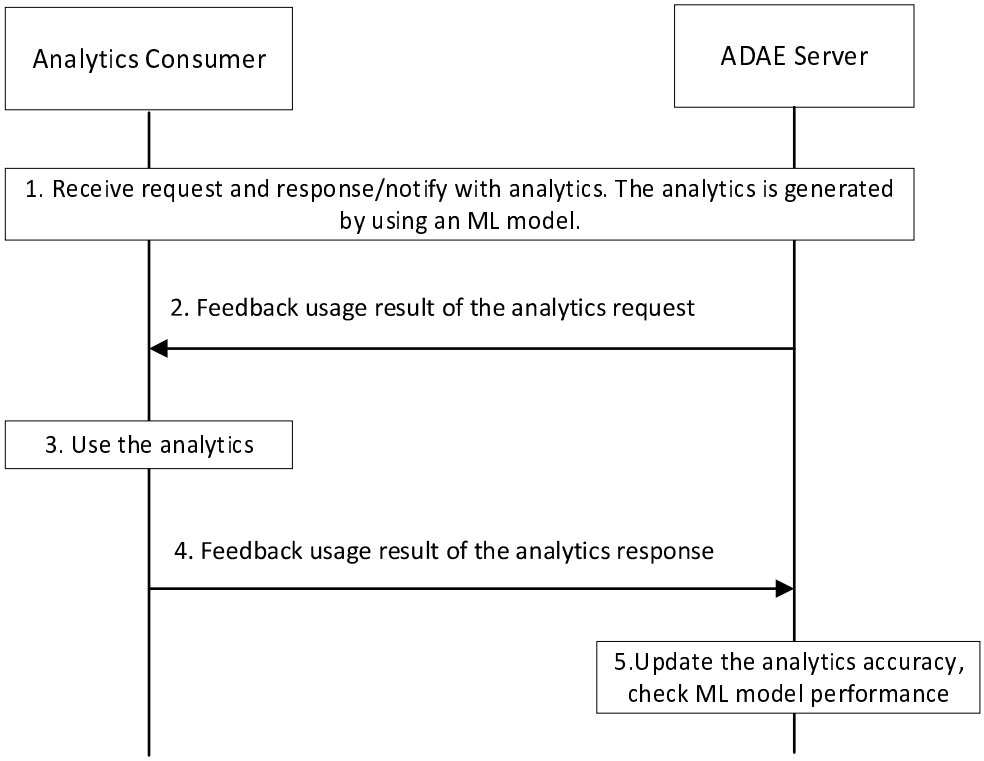

Figure 8.19.2-1: ADAES supports for ML model performance degradation detection

1. The ADAE Server receives a request from the consumer for analytics, generates analytics by using the ML model provided by AIMLE Server, and responds/notifies to the consumer with the required analytics.
2. The ADAE Server requests the consumer to provide feedback on the usage of the analytics.
3. The consumer uses the analytics for its operations and collects operation results. Performance degradation may be found from the operation results. The performance degradation may be caused by e.g., insufficient analytics accuracy, or the current analytics cannot fulfill the changed conditions at the consumer.
4. The consumer provides feedback on the result of usage of the analytics to the ADAE Server.
5. The ADAE Server updates the analytics accuracy based on feedback information from the consumer, and checks the performance of the ML model, which is used to generate the analytics, e.g., performance degradation of the ML model.

9 ADAE layer APIs

9.1 General

The following ADAE capabilities are offered as APIs:

- ADAE server APIs;
- A-ADRF APIs;

The following SEAL service APIs are specified in 3GPP TS 23.434 [2] (and TS 23.435 [6] for NSCE):

- Group management server APIs;
- Location management server APIs;
- Configuration management server APIs;
- Identity management server APIs;

- Key management server APIs; and
- Network slice capability enablement APIs.

9.2 ADAE server APIs

9.2.1 General

This clause provides the APIs provided by ADAES.

9.2.2 ADAE server APIs

Table 9.2.2-1 illustrates the ADAE server APIs.

Table 9.2.2-1: List of ADAE server APIs

API Name	API Operations	Known Consumer(s)	Communication Type
SS_ADAE_VAL_performance_analytics	Subscribe	VAL server	Subscribe/Notify
	Notify		
SS_ADAE_slice_performance_analytics	Subscribe	VAL server	Subscribe/Notify
	Notify		
SS_ADAE_UE-to-UE_performance_analytics	Subscribe	VAL server	Subscribe/Notify
	Notify		
SS_ADAE_server-to-server_performance_analytics	Subscribe	VAL server / EES	Subscribe/Notify
	Notify		
SS_ADAE_location_accuracy_analytics	Subscribe	VAL server	Subscribe/Notify
	Notify		
SS_ADAE_service_API_analytics	Subscribe	VAL server / Subscriber/ API invoker	Subscribe/Notify
	Notify		
SS_ADAE_slice_usage_pattern_analytics	Subscribe	VAL server / SEAL server	Subscribe/Notify
	Notify		
SS_ADAE_edge_analytics	Subscribe	VAL server / EAS / EES	Subscribe/Notify
	Notify		
	Get	VAL server / EAS / EES	Request / Response
SS_ADAES_slice_usage_stats	Get	VAL server	Request / Response
SS_ADAES_edge_preparation_analytics	Subscribe	VAL server / ECS / EES	Subscribe/Notify
	Notify		
	Get	VAL server / ECS / EES	Request / Response
SS_ADAE_collision_detection_analytics	Subscribe	VAL server / LM server / UAE server, UAS application specific server	Subscribe/Notify
	Notify		
	Get	VAL server / LM server / UAE server, UAS application specific server	Request / Response
SS_ADAE_location-related_UE_group_analytics	Subscribe	LM server	Subscribe/Notify
	Notify		
	Get	LM server	Request / Response
SS_ ADAE_AIML_member_capability_analytics	Subscribe	VAL server / AIMLE server	Subscribe/Notify
	Notify		
	Get	VAL server / AIMLE server	Request / Response
SS_ ADAE_ServiceExp	Request	ADAE client	Request / Response
SS_ADAE_DN_energy_analytics	Get	VAL server / EAS / EES	Request / Response

9.2.3 SS_ ADAE_VAL_performance_analytics API

9.2.3.1 General

API description: This API enables the VAL server to communicate with the ADAE server for subscribing for VAL performance analytics and for getting notified on the result.

9.2.3.2 Subscribe

API operation name: VAL_performance_analytics_subscribe

Description: The consumer subscribes for VAL performance analytics.

Inputs: See clause 8.2.4.2.

Outputs: See clause 8.2.4.3.

See clause 8.2.2 and 8.2.3 for details of usage of this operation.

9.2.3.3 Notify

API operation name: VAL_performance_analytics_notify

Description: The consumer is notified by ADAES on the VAL performance analytics.

Inputs: -

Outputs: See clause 8.2.4.7.

See clause 8.2.2 and 8.2.3 for details of usage of this operation.

9.2.4 SS_ ADAE_slice_performance_analytics API

9.2.4.1 General

API description: This API enables the VAL server to communicate with the ADAE server for subscribing for slice specific application performance analytics and for getting notified when analytics are derived.

9.2.4.2 Subscribe

API operation name: slice_performance_analytics_subscribe

Description: The consumer subscribes for slice specific performance analytics.

Inputs: See clause 8.3.3.2.

Outputs: See clause 8.3.3.3.

See clause 8.3.2 for details of usage of this operation.

9.2.4.3 Notify

API operation name: slice_performance_analytics_notify

Description: The consumer is notified by ADAES on the slice specific performance analytics.

Inputs: -

Outputs: See clause 8.3.3.4.

See clause 8.3.2 for details of usage of this operation.

9.2.5 SS_ ADAE_UE-to-UE_performance_analytics API

9.2.5.1 General

API description: This API enables the VAL server to communicate with the ADAE server for subscribing for UE-to-UE session performance analytics and for getting notified when analytics are derived.

9.2.5.2 Subscribe

API operation name: UE-to-UE performance_analytics_subscribe

Description: The consumer subscribes for UE-to-UE performance analytics.

Inputs: See clause 8.4.3.2.

Outputs: See clause 8.4.3.3.

See clause 8.4.2 for details of usage of this operation.

9.2.5.3 Notify

API operation name: UE-to-UE performance_analytics_notify

Description: The consumer is notified by ADAES on the slice specific performance analytics.

Inputs: -

Outputs: See clause 8.4.3.6.

See clause 8.4.2 for details of usage of this operation.

9.2.6 SS_ ADAE_location_accuracy_analytics API

9.2.6.1 General

API description: This API enables the VAL server to communicate with the ADAE server for subscribing for location accuracy analytics and for getting notified when analytics are derived.

9.2.6.2 Subscribe

API operation name: Location_accuracy_analytics_subscribe

Description: The consumer subscribes for location accuracy analytics.

Inputs: See clause 8.5.3.2.

Outputs: See clause 8.5.3.3.

See clause 8.5.2 for details of usage of this operation.

9.2.6.3 Notify

API operation name: Location_accuracy_analytics_notify

Description: The consumer is notified by ADAES on the location accuracy analytics.

Inputs: -

Outputs: See clause 8.5.3.6.

See clause 8.5.2 for details of usage of this operation.

9.2.7 SS_ ADAE_service_API_analytics API

9.2.7.1 General

API description: This API enables the VAL server to communicate with the ADAE server for subscribing for service API analytics and for getting notified when analytics are derived.

9.2.7.2 Subscribe

API operation name: Service_API_analytics_subscribe

Description: The consumer subscribes for service API analytics.

Inputs: See clause 8.6.3.2.

Outputs: See clause 8.6.3.3.

See clause 8.6.2 for details of usage of this operation.

9.2.6.3 Notify

API operation name: Service_API_analytics_notify

Description: The consumer is notified by ADAES on the location accuracy analytics.

Inputs: -

Outputs: See clause 8.6.3.6.

See clause 8.6.2 for details of usage of this operation.

9.2.8 SS_ADAE_slice_usage_pattern_analytics API

9.2.8.1 General

API description: This API enables the VAL server to communicate with the ADAE server for subscribing for slice usage pattern analytics and for getting notified when analytics are derived.

9.2.8.2 Subscribe

API operation name: slice_usage_pattern_analytics_subscribe

Description: The consumer subscribes for slice usage pattern analytics.

Inputs: See clause 8.7.3.2.

Outputs: See clause 8.7.3.3.

See clause 8.7.2 for details of usage of this operation.

9.2.8.3 Notify

API operation name: slice_usage_pattern_analytics_notify

Description: The consumer is notified by ADAES on the slice usage pattern analytics.

Inputs: -

Outputs: See clause 8.7.3.4.

See clause 8.7.2 for details of usage of this operation.

9.2.9 SS_ ADAE_edge_analytics API

9.2.9.1 General

API description: This API enables the VAL server to communicate with the ADAE server for subscribing for edge load analytics and for getting notified when analytics are derived.

9.2.9.2 Subscribe

API operation name: edge_analytics_subscribe

Description: The consumer subscribes for edge load analytics.

Inputs: See clause 8.8.3.2.

Outputs: See clause 8.8.3.3.

See clause 8.8.2 for details of usage of this operation.

9.2.9.3 Notify

API operation name: edge_analytics_notify

Description: The consumer is notified by ADAES on the edge load analytics.

Inputs: -

Outputs: See clause 8.8.3.7.

See clause 8.8.2.1 for details of usage of this operation.

9.2.9.4 Get

API operation name: edge_analytics_get

Description: The consumer requests edge analytics data.

Inputs: See clause 8.8.3.8.

Outputs: See clause 8.8.3.9.

See clause 8.8.2.2 for details of usage of this operation.

9.2.10 SS_ ADAE_slice_usage_stats

9.2.10.1 General

API description: This API enables the Consumer to communicate with the ADAE server for requesting and receiving slice usage statistical data.

9.2.10.2 Get

API operation name: slice_usage_stats_get

Description: The consumer requests and receives slice usage statistics from ADAE server.

Inputs: See clause 8.7.4.7.

Outputs: See clause 8.7.4.8.

See clause 8.7.3 for details of usage of this operation.

9.2.11 SS_ADAE_edge_preparation_analytics API

9.2.11.1 General

API description: This API enables the analytics consumer (e.g., the VAL server, ECS, EES) to communicate with the ADAE server for requesting or subscribing to edge computing preparation.

9.2.11.2 Subscribe

API operation name: edge_preparation_analytics_subscribe

Description: The consumer subscribes for edge computing preparation analytics.

Inputs: See clause 8.11.3.2.

Outputs: See clause 8.11.3.3.

See clause 8.11.2.1 for details of usage of this operation.

9.2.11.3 Notify

API operation name: edge_preparation_analytics_notify

Description: The consumer is notified by the ADAE server on the edge computing preparation analytics.

Inputs: -

Outputs: See clause 8.11.3.4.

See clause 8.112.1 for details of usage of this operation.

9.2.11.4 Get

API operation name: edge_preparation_analytics_get

Description: The consumer requests edge computing preparation analytics

Inputs: -See clause 8.11.3.7

Outputs: See clause 8.11.3.8.

See clause 8.11.2.2 for details of usage of this operation.

9.2.12 SS_ADAE_server-to-server_performance_analytics API

9.2.12.1 General

API description: This API enables the analytics consumer (e.g., the VAL server, EES) to communicate with the ADAE server for requesting or subscribing to server-to-server performance analytics.

9.2.12.2 Subscribe

API operation name: server-to-server_performance_analytics_subscribe

Description: The consumer subscribes to the ADAE server for Server-to-server performance analytics.

Inputs: See clause 8.13.3.2.

Outputs: See clause 8.13.3.3.

See clause 8.13.2.1 for details of usage of this operation.

9.2.12.3 Notify

API operation name: server-to-server_performance_analytics_notify

Description: The consumer is notified by the ADAE server on the Server-to-server performance analytics.

Inputs: -

Outputs: See clause 8.13.3.4.

See clause 8.13.2.1 for details of usage of this operation.

9.2.13 SS_ADAE_collision_detection_analytics API

9.2.13.1 General

API description: This API enables the analytics consumer (e.g. VAL Server, LM Server, UAE server, UAS application specific server) to communicate with the ADAE server for requesting or subscribing to collision detection analytics.

9.2.13.2 Subscribe

API operation name: collision_detection_analytics_subscribe

Description: The consumer subscribes for collision detection analytics.

Inputs: See clause 8.14.3.2.

Outputs: See clause 8.14.3.3.

See clause 8.14.2.1 for details of usage of this operation.

9.2.13.3 Notify

API operation name: collision_detection_analytics_notify

Description: The consumer is notified by the ADAE server on collision detection analytics.

Inputs: -

Outputs: See clause 8.14.3.4.

See clause 8.14.2.1 for details of usage of this operation.

9.2.13.4 Get

API operation name: collision_detection_analytics_get

Description: The consumer requests collision detection analytics.

Inputs: See clause 8.14.3.8.

Outputs: See clause 8.14.3.9.

See clause 8.14.2.2 for details of usage of this operation.

9.2.14 SS_ADAE_location-related_UE_group_analytics API

9.2.14.1 General

API description: This API enables the analytics consumer (e.g. LMS) to communicate with the ADAE server for requesting or subscribing to location-related UE group analytics.

9.2.14.2 Subscribe

API operation name: location-related_UE_group_analytics_subscribe

Description: The consumer subscribes for location-related UE group analytics.

Inputs: See clause 8.15.3.2.

Outputs: See clause 8.15.3.3.2.

See clause 8.15.2.1 for details of usage of this operation.

9.2.14.3 Notify

API operation name: location-related_UE_group_analytics_notify

Description: The consumer is notified by the ADAE server on location-related UE group analytics.

Inputs: -

Outputs: See clause 8.15.3.4.

See clause 8.15.2.1 for details of usage of this operation.

9.2.14.4 Get

API operation name: location-related_UE_group_analytics_get

Description: The consumer requests location-related UE group analytics.

Inputs: -See clause 8.15.3.8

Outputs: See clause 8.15.3.9.

See clause 8.15.2.2 for details of usage of this operation.

9.2.15 SS_ADAE_AIML_member_capability_analytics API

9.2.15.1 General

API description: This API enables the analytics consumer (e.g. VAL Server, AIMLE Server) to communicate with the ADAE server for requesting or subscribing to application layer AIML member capability analytics.

9.2.15.2 Subscribe

API operation name: AIML_member_capability_analytics_subscribe

Description: The consumer subscribes for application layer AIML member capability analytics.

Inputs: See clause 8.16.3.2.

Outputs: See clause 8.16.3.3.

See clause 8.16.2.1 for details of usage of this operation.

9.2.15.3 Notify

API operation name: AIML_member_capability_analytics_notify

Description: The consumer is notified by the ADAE server on application layer AIML member capability analytics.

Inputs: -

Outputs: See clause 8.16.3.4.

See clause 8.16.2.1 for details of usage of this operation.

9.2.15.4 Get

API operation name: AIML_member_capability_analytics_get

Description: The consumer requests application layer AIML member capability analytics.

Inputs: -See clause 8.16.3.8

Outputs: See clause 8.16.3.9.

See clause 8.16.2.2 for details of usage of this operation.

9.2.16 SS_ ADAE_ServiceExp API

9.2.16.1 General

API description: This API enables the ADAE client share service experience information to ADAE server.

9.2.16.2 Request

API operation name: SS_ ADAE_ServiceExp_Request

Description: The consumer sends application service experience report to the server.

Inputs: See clause 8.9.3.1.

Outputs: See clause 8.9.3.2

See clause 8.9.2.1 for details of usage of this operation.

9.2.17 SS_ ADAE_DN_energy_analytics API

9.2.17.1 General

API description: This API enables the VAL server to communicate with the ADAE server for requesting for DN energy efficiency/consumption analytics.

9.2.17.2 Get DN_energy_analytics

API operation name: DN_energy_analytics_get

Description: The consumer requests DN energy efficiency/consumption analytics.

Inputs: See clause 8.18.3.2.

Outputs: See clause 8.18.3.3.

See clause 8.18.2 for details of usage of this operation.

9.3 A-ADRF APIs

9.3.1 General

This clause provides the APIs provided by A-ADRF.

9.3.2 A-ADRF APIs

Table 9.3.2-1 illustrates the A-ADRF APIs.

Table 9.3.2-1: List of A-ADRF APIs

API Name	API Operations	Known Consumer(s)	Communication Type
SS_AADRF_Data_Collection	Subscribe	ADAES	Subscribe / Notify
	Notify		
SS_ AADRF_Historical_ServiceAPI_Logs	Get	ADAES	Request / Response
SS_AADRF_NetworkSlice_Data	Get	ADAES	Request / Response
SS_AADRF_Location_Accuracy_Data	Get	ADAES	Request / Response
SS_AADRF_EdgeData_Collection	Subscribe	ADAES	Subscribe / Notify
	Notify	ADAES	
SS_AADRF_Edge_Preparation_Data	Get	ADAES	Request / Response
SS_AADRF_Data_Storage	Request Subscription	ADAE server, A-DCCF	Request / Response
	Store Data	ADAE server	Request / Response
SS_AADRF_ServerToServer_Analytics	Get	ADAES	Request / Response

9.3.3 SS_AADRF_Data_Collection API

9.3.3.1 General

API description: This API enables the ADAE server to communicate with the A-ADRF for subscribing for offline data collection and for getting notified about the offline data/statistics.

9.3.3.2 Subscribe

API operation name: Data_Collection_Subscribe

Description: The consumer subscribes for offline data from A-ADRF.

Inputs: See clause 8.2.4.4.

Outputs: See clause 8.2.4.5.

See clause 8.2.2 for details of usage of this operation.

9.3.3.3 Notify

API operation name: Data_Collection_Notify

Description: The consumer is receiving the offline data from A-ADRF as notification, based on subscription.

Inputs: -

Outputs: See clause 8.2.4.6.

See clause 8.2.2 for details of usage of this operation.

9.3.4 SS_ AADRF_Historical_serviceAPI_logs API

9.3.4.1 General

API description: This API enables the ADAE server to communicate with the A-ADRF for requesting service API logs and receiving the offline data/statistics on API logs.

9.3.4.2 Get

API operation name: Historical_ServiceAPI_Logs_Get

Description: The consumer requests API logs from A-ADRF.

Inputs: See clause 8.6.3.4.

Outputs: See clause 8.6.3.5.

See clause 8.6.2 for details of usage of this operation.

9.3.5 SS_ AADRF_NetworkSlice_data API

9.3.5.1 General

API description: This API enables the ADAE server to communicate with the A-ADRF for requesting and receiving network slice data.

9.3.5.2 Get

API operation name: NetworkSlice_Data_Get

Description: The consumer requests network slice data from A-ADRF.

Inputs: See clause 8.7.3.5.

Outputs: See clause 8.7.3.6.

See clause 8.7.2 for details of usage of this operation.

9.3.6 SS_AADRF_EdgeData_Collection API

9.3.6.1 General

API description: This API enables the ADAE server to communicate with the A-ADRF for subscribing for edge data collection and for getting notified about the offline data/statistics for the EDN and/or EAS/EES.

9.3.6.2 Subscribe

API operation name: EdgeData_Collection_Subscribe

Description: The consumer subscribes for offline edge data from A-ADRF.

Inputs: See clause 8.8.3.4.

Outputs: See clause 8.8.3.5.

See clause 8.8.2 for details of usage of this operation.

9.3.6.3 Notify

API operation name: EdgeData_Collection_Notify

Description: The consumer is receiving the offline edge data from A-ADRF as notification, based on subscription.

Inputs: -

Outputs: See clause 8.8.3.6.

See clause 8.8.2 for details of usage of this operation.

9.3.7 SS_AADRF_Location_Accuracy API

9.3.7.1 General

API description: This API enables the ADAE server to communicate with the A-ADRF to request location analytics/data for VAL UEs or VAL service area.

9.3.7.2 Get

API operation name: Location_Accuracy_Data_Get

Description: The consumer is receiving offline location analytics/data from A-ADRF.

Inputs: See clause 8.5.3.4.

Outputs: See clause 8.5.3.5.

See clause 8.5.2 for details of usage of this operation.

9.3.8 SS_AADRF_Edge_Preparation_Data API

9.3.8.1 General

API description: This API enables the ADAE server to communicate with the A-ADRF to request edge computing preparation data for the EAS, EES, and/or ECS.

9.3.8.2 Get

API operation name: edge_preparation_data_get

Description: The consumer is receiving offline edge computing preparation data from the A-ADRF.

Inputs: See clause 8.11.3.5.

Outputs: See clause 8.11.3.6.

See clause 8.11.2.1 for details of usage of this operation.

9.3.9 SS_AADRF_Data_Storage API

9.3.9.1 General

API description: This API enables the ADAE server or the A-DCCF to request the A-ADRF to initiate a subscription for data or analytics. Data or analytics provided in notifications as a result of the subsequent subscription by the A-ADRF are stored in the A-ADRF. This API also enables the consumer to request the A-ADRF to store data or analytics from ADAE server or A-DCCF.

9.3.9.2 Request Subscripiton

API operation name: Data_Storage_Subscribe

Description: The consumer requests A-ADRF to subscribe for data or analytics from ADAE server or A-DCCF for store. This service operation provides parameters needed by the A-ADRF to initiate the subscription (to an ADAE server or A-DCCF).

Inputs: See clause 8.10.3.2.

Outputs: See clause 8.10.3.3.

See clause 8.10.2 for details of usage of this operation.

9.3.9.3 Store Data

API operation name: Data_Storage_Request

Description: The consumer requests A-ADRF to store data or analytics from ADAE server or A-DCCF. Data or analytics are provided to the A-ADRF in the request message.

Inputs: See clause 8.10.3.4.

Outputs: See clause 8.10.3.5.

See clause 8.10.2 for details of usage of this operation.

9.3.10 SS_AADRF_ServerToServer_Analytics API

9.3.10.1 General

API description: This API enables the ADAE server to communicate with the A-ADRF to request server-to-server analytics for inter-server communication.

9.3.10.2 Get

API operation name: ServerToServer_Analytics_Get

Description: The consumer is receiving offline server-to-server analytics/data from A-ADRF.

Inputs: See clause 8.13.3.7.

Outputs: See clause 8.13.3.8.

See clause 8.13.2 for details of usage of this operation.

9.4 A-DCCF APIs

9.4.1 General

This clause provides the APIs provided by A-DCCF.

9.4.2 A-DCCF APIs

Table 9.4.2-1 illustrates the A-DCCF APIs.

Table 9.4.2-1: List of A-DCCF APIs

API Name	API Operations	Known Consumer(s)	Communication Type
SS_ADCCF_Data_Collection	Subscribe	ADAE server	Subscribe / Notify
	Notify		
	Get	ADAE server	Request / Response

9.4.3 SS_ADCCF_Data_Collection API

9.4.3.1 General

API description: This API enables the consumer to subscribe/unsubscribe for data or analytics via the A-DCCF, be notified about data or analytics exposed by the A-DCCF, fetch the subscribed data and have data delivered via the A-DCCF. Historical data, or runtime data may be obtained using this service.

When the subscription is accepted by the A-DCCF, the consumer (ADAE server) receives from the A-DCCF an identifier (Subscription Correlation ID) allowing it to further manage (modify, delete) the subscription.

NOTE: The definition of delete service operation is within stage 3 scope.

9.4.3.2 Subscribe

API operation name: Data_Collection_Subscribe

Description: The consumer subscribes to receive data or analytics, or if the data is already requested from the A-DCCF, then the subscription is updated. The subscription includes service operation specific parameters that identify the data or analytics to be provided. The consumer may also request that data be stored in an A-ADRF. When historical data is being obtained, the consumer may specify the A-ADRF ID.

Inputs: See clause 8.12.3.2.

Outputs: See clause 8.12.3.3.

See clause 8.12.2 for details of usage of this operation.

9.4.3.3 Notify

API operation name: Data_Collection_Notify

Description: The A-DCCF notifies the consumer of the requested data or analytics according to the request, or notifies of the availability of previously subscribed data or analytics when data delivery is via the A-DCCF. The A-DCCF may also notify the consumer when data or analytics is to be deleted.

Inputs: See clause 8.12.3.4.

Outputs: -.

See clause 8.12.2 for details of usage of this operation.

9.4.3.4 Request

API operation name: Data_Collection_Request

Description: The consumer retrieves data or analytics from the A-DCCF.

Inputs: See clause 8.12.3.5.

Outputs: See clause 8.12.3.6.

See clause 8.12.2 for details of usage of this operation.

10 Analytics related to satellite access

10.1 General

This clause describes the procedures and information flows for analytics related to satellite access.

10.2 Support for UE RAT connectivity analytics

10.2.1 General

This clause describes the procedure for supporting UE RAT connectivity analytics for satellite access. The ADAES service consumer can subscribe and receive notifications about UE RAT connectivity analytics events. This analytics helps to predict the type of satellite RAT that a UE will latch onto on a particular location and/or particular time and helps the analytics consumer to decide on the actions to improve the service experience over the satellite access.

10.2.2 Procedure

Figure 10.2.2-1 illustrates the procedure for UE RAT connectivity analytics.

Pre-conditions:

1. The ADAES is registered and capable of interacting with 5GS to UE mobility analytics.

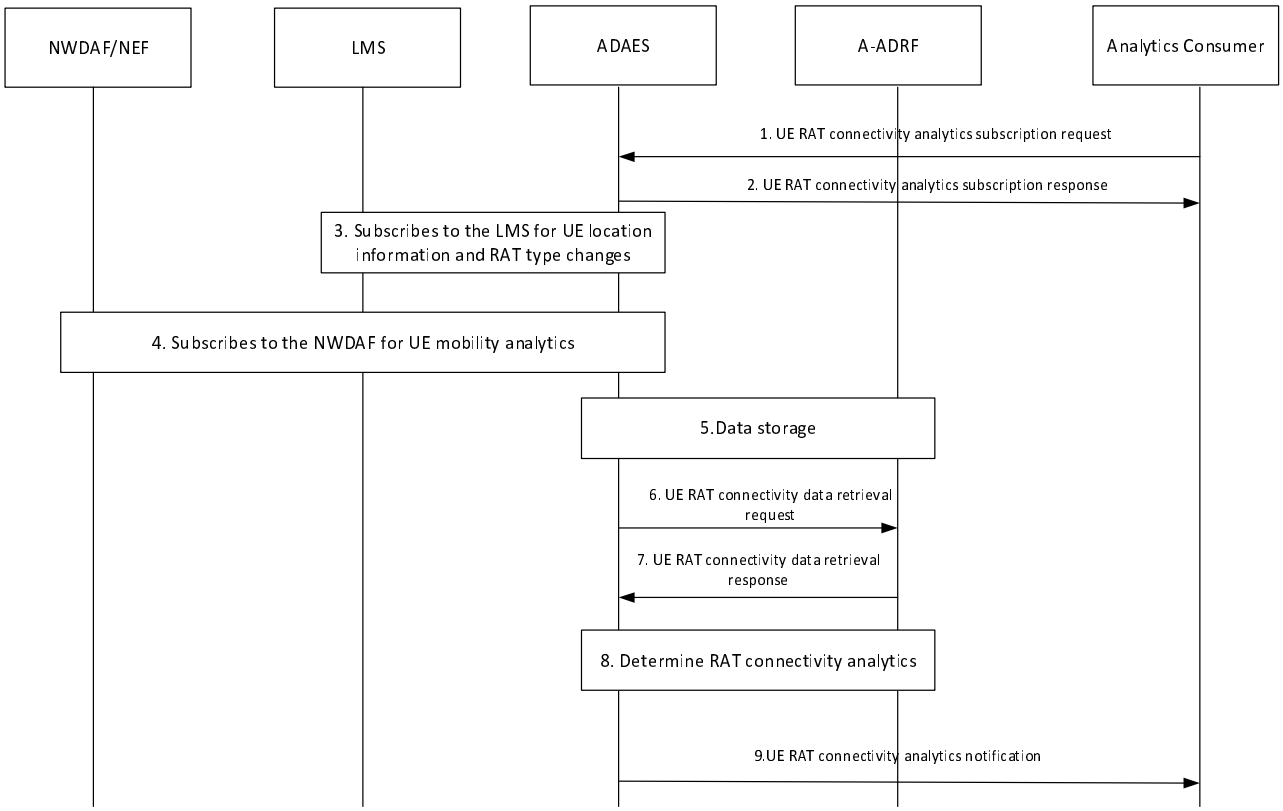

Figure 10.2.2-1: Procedure for supporting UE RAT connectivity analytics

1. The analytics consumer (e.g.VAL server) makes a subscription request to ADAE server for UE RAT connectivity prediction/stats, including an analytics event ID for UE RAT Connectivity analytics. The request may include also the target area, a target VAL service, or a VAL UE, or group of UEs of the VAL service, time validity. If the VAL UEs are provided by the VAL server, this request may also include the expected route or a set of waypoints for the UEs of the VAL application.

2. The ADAE server sends a UE RAT connectivity analytics subscription response as an ACK to the VAL server.

3. The ADAE server subscribes to the SEAL Location management server to get the location information of the VAL UE along with the RAT type. It can set the trigger criteria of receiving the location information of the UE whenever UE RAT type changes as specified in 3GPP TS 23.434 [2] clause 9.3.5.

4. The ADAE server subscribes for NWDAF UE mobility analytics per VAL UE (for all the VAL UEs) and gets notification on the per UE location/mobility analytics based on 3GPP TS 23.288 [4] clause 6.7.2.

5. If the data is collected from multiple sources, the ADAES combines or correlates the data/analytics from steps 3-4 and stores the data into A-ADRF if needed.

6. The ADAE server optionally requests UE RAT connectivity historical analytics/data from A-ADRF for the corresponding VAL UEs.

7. Based on the request, the ADAE server receives UE RAT connectivity historical analytics/data from A-ADRF for the corresponding VAL UEs.

8. The ADAE server abstracts or correlates the data/analytics from steps 5-6 and provides analytics on the UE RAT connectivity for the target VAL application.

9. The ADAE server sends the UE RAT connectivity analytics notification to the consumer.

10.2.3 Information flows

10.2.3.1 UE RAT connectivity analytics subscription request

Table 10.2.3.1-1 describes information elements for the UE RAT connectivity analytics subscription request from the VAL server/Analytics consumer to the ADAE server.

Table 10.2.3.1-1

Information element	Status	Description
VAL server ID	M	The identifier of the VAL server.
Analytics ID	M	The identifier of the UE RAT connectivity analytics event.
VAL UE ID(s) or Group ID	M	The identity of the VAL UE(s) or group of UEs for which the analytics subscription applies
VAL service ID	O	The identifier of the VAL service for which location accuracy analytics is requested.
Preferred confidence level	O	The level of accuracy for the analytics service (in case of prediction).
Area of Interest	O	The geographical or service area for which the subscription request applies.
Time validity	O	The time validity of the subscription request.
UE mobility / route information	O	Information on the target UE or group UE mobility including the expected route/set of waypoints.
Reporting requirements	O	It describes the requirements for analytics reporting. This requirement may include e.g. the type and frequency of reporting (periodic or event triggered), the reporting periodicity in case of periodic, and reporting thresholds.

10.2.3.2 UE RAT Connectivity analytics subscription response

Table 10.2.3.2-1 describes information elements for the UE RAT connectivity analytics subscription response from the ADAE server to the VAL server/Analytics consumer.

Table 10.2.3.2-1

Information element	Status	Description
Result	M	The result of the analytics subscription request (positive or negative acknowledgement)

10.2.3.3 UE RAT Connectivity data retrieval request

Table 10.2.3.3-1 describes information elements for the UE RAT connectivity data retrieval request from the ADAE server to the A-ADRF.

Table 10.2.3.3-1

Information element	Status	Description
ADAE server ID	M	The identifier of the ADAE server
Analytics ID	M	The identifier of the analytics event i.e. UE RAT connectivity analytics
List of VAL UE IDs and addresses	M	The VAL UE(s) identifiers and IP address(es) for which the data/analytics apply
VAL service ID	O	The service ID, in case of requesting historical data for a particular VAL service.
Reporting configuration	O	The configuration for data reporting. This requirement may include e.g. the frequency of reporting (periodic), the reporting periodicity in case of periodic, and reporting thresholds, whether data abstraction is needed or not.
Data collection requirements	O	The requirements for data collection, including the format of data, frequency of reporting, level of abstraction of data, level of accuracy of data.
Area of Interest	O	The geographical or service area for which the subscription request applies
Time validity	O	The time validity of the request

10.2.3.4 UE RAT Connectivity data retrieval response

Table 10.2.3.4-1 describes information elements for the UE RAT connectivity data retrieval response from the A-ADRF to the ADAE server.

Table 10.2.3.4-1

Information element	Status	Description
Analytics ID	M	The identifier of the analytics event.
List of VAL UE IDs and addresses	M	The VAL UE(s) identifiers and IP address(es) for which the analytics apply
VAL service ID	O	The service ID, in case of requesting historical data for a particular VAL service.
Analytics Output	M	The reported analytics for the UE RAT connectivity, which can be in form of offline stats/historical data for a specific VAL service or for particular UE(s) or group of UEs

10.2.3.5 UE RAT Connectivity analytics notification

Table 10.2.3.5-1 describes information elements for the UE RAT connectivity analytics notification from the A-ADRF to the ADAE server.

Table 10.2.3.5-1

Information element	Status	Description
Analytics ID	M	The identifier of the analytics event (UE RAT connectivity)
VAL UE ID(s)	O	The identity of the VAL UE(s) for which the analytics applies.
VAL service ID	O	The identifier of the VAL service for which the analytics applies.
Analytics Output	M	The analytics output which can be predictive or statistical parameter.
> RAT type prediction for given waypoints	O	A predicted or expected RAT type changes for a particular VAL service or UEs for the given waypoints.
>> Applicable area	O	The set of location co-ordinates or waypoints for which the analytics output is applicable.
>> Applicable time period	O	The time period that the analytics applies to.
Confidence level	O	For predictive analytics, the achieved confidence level can be provided.
> RAT type prediction for a given time period	O	A predicted or expected RAT type changes for a particular VAL service or UEs for the given time period.
>> Applicable time period	O	The time period that the analytics applies to.
>> Confidence level	O	For predictive analytics, the achieved confidence level can be provided.

10.2.4 ADAE server APIs

10.2.4.1 General

This clause provides the APIs provided by ADAES related to satellite access.

10.2.4.2 ADAE server APIs

Table 10.2.4.2-1 illustrates the ADAE server APIs related to satellite access.

Table 10.2.4.2-1: List of ADAE server APIs

API Name	API Operations	Known Consumer(s)	Communication Type
SS_ADAE_UE_RAT_connectivity_analytics	Subscribe	VAL server	Subscribe/Notify
	Notify		

10.2.4.3 SS_ADAE_UE_RAT_connectivity_analytics API

10.2.4.3.1 General

API description: This API enables the analytics consumer (e.g., the VAL server) to communicate with the ADAE server for requesting or subscribing to UE RAT connectivity analytics.

10.2.4.3.2 Subscribe

API operation name: UE_RAT_connectivity_analytics_subscribe

Description: The consumer subscribes to the ADAE server for UE RAT connectivity analytics.

Inputs: See clause 10.2.3.1.

Outputs: See clause 10.2.3.2.

See clause 10.2.2 for details of usage of this operation.

10.2.4.3.3 Notify

API operation name: UE_RAT_connectivity_analytics_notify

Description: The consumer is notified by the ADAE server on the Server-to-server performance analytics.

Inputs: -

Outputs: See clause 10.2.3.5.

See clause 10.2.2 for details of usage of this operation.

10.2.5 A-ADRF APIs

10.2.5.1 General

This clause provides the APIs provided by A-ADRF related to satellite access.

10.2.5.2 A-ADRF APIs

Table 10.2.5.2-1 illustrates the A-ADRF APIs related to satellite access.

Table 10.2.5.2-1: List of A-ADRF APIs

API Name	API Operations	Known Consumer(s)	Communication Type
SS_ADRF_UE_RAT_connectivity_analytics	Get	ADAES	Request/Response

10.2.5.3 SS_AADRF_UE RAT connectivity analytics API

10.2.5.3.1 General

API description: This API enables the ADAE server to communicate with the A-ADRF to request UE RAT connectivity analytics of VAL UEs.

10.2.5.3.2 Get

API operation name: UE_RAT_connectivity_analytics_Data_Get

Description: The consumer is receiving offline UE RAT connectivity analytics/data from A-ADRF.

Inputs: See clause 10.2.3.3.

Outputs: See clause 10.2.3.4.

See clause 10.2.2 for details of usage of this operation.

Annex A (informative): Deployment scenarios

A.1 General

This clause provides the different deployment models for ADAE services. There could be three deployment options:

- ADAES can be deployed at a centralized cloud platform, and collects data from multiple EDNs
- ADAES can be deployed at the edge platform
- Coordinated ADAES deployment, where multiple ADAE services are deployed in edge or central clouds. Such deployment allows for local-global analytics for system wide optimization

A.2 Deployment model #1: Cloud-deployed ADAES

In this deployment, as shown in Figure A.2-1, the ADAES is centrally located and can provide analytics services to different consumers including, edge servers, VAL servers, as well as to other SEAL servers (e.g. NSCE).

The statistics/predictions that the ADAES provides are applicable to the ADAES service area, which can be provided for the entire PLMN.

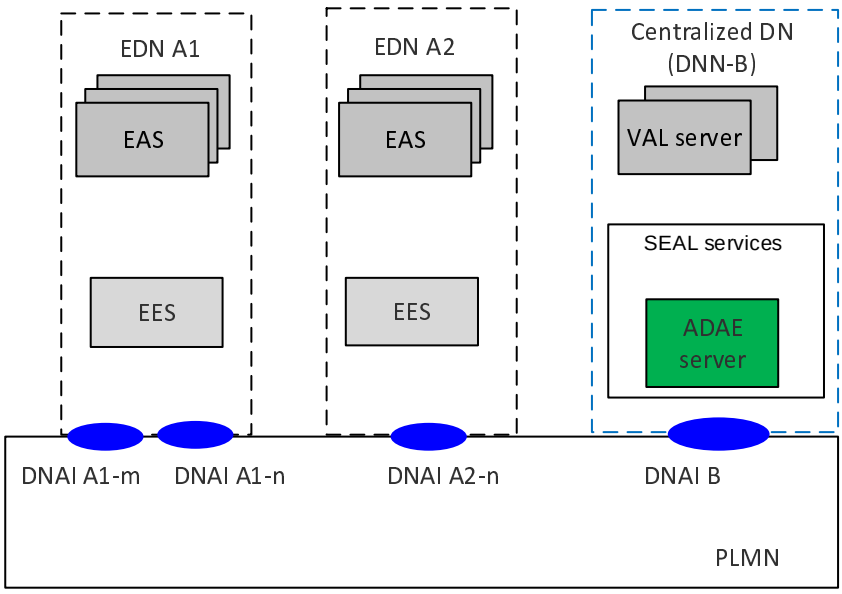

Figure A.2-1: Cloud deployed ADAES

A.3 Deployment model #2 Edge-deployed ADAES

In this deployment, as shown in Figure A.3-1, the ADAES is located at the EDN and provides analytics services to the EAS and EES at the edge platform. ADAES can be deployed by the ECSP or the MNO to provide analytics for the application or edge parameters.

The statistics/predictions that the edge deployed ADAES are applicable to the ADAES service areas (as shown in the example in Fig A.2-2), which are equivalent to the EES/EAS service areas. Such analytics can be about the edge load or the EAS performance and can be provided to consumers within EDN.

In this deployment the interaction between edge deployed ADAES is possible for exchanging edge/application analytics for application mobility scenarios or for cases when ADAES #1 and #2 service areas have overlapping coverage.

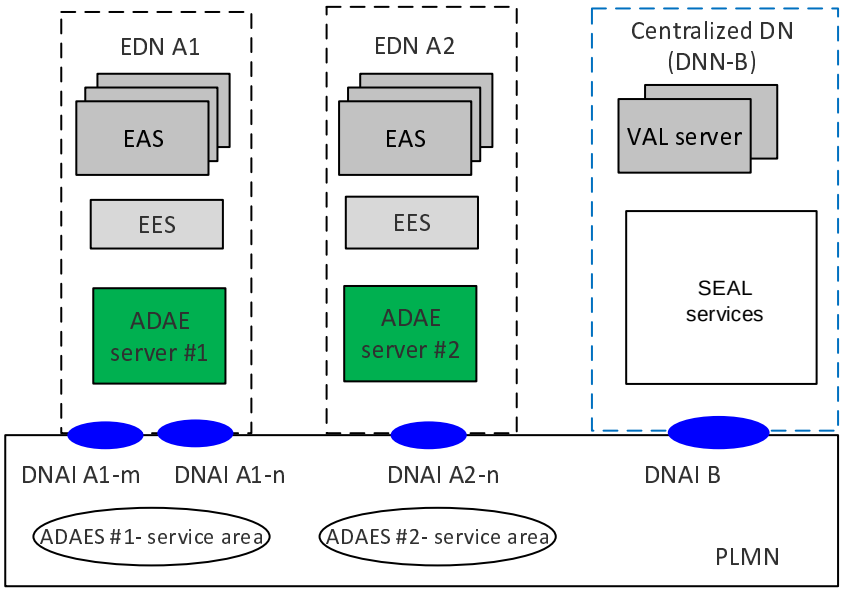

Figure A.3-1: Edge deployed ADAES

A.4 Deployment model #3: Coordinated ADAES deployment

In this deployment, multiple ADAESs can be located at different EDNs/DNs and can be deployed by the same ADAE provider. Such coordinated deployments allow the local – global analytics derivation (which may be needed for improving the analytics confidence level). The centrally deployed ADAES can also act as ADAE analytics aggregator entity and configures the edge deployed ADAES to derive analytics on different sub-areas.

One example is the use of analytics for the EDN#1 or EDN#2 load which will help predicting the VAL server performance at a centrally located ADAES. Such deployment is also applicable for ML-based analytics methods, like supervised learning, where the centrally located ADAES acts as ML model training entity, and the edge located ADAESs can act as ML model inference entities (using edge data to improve the prediction accuracy).

The statistics/predictions that the edge deployed ADAES correspond to the ADAES service areas (as shown in the example in Fig A.4-1), which is equivalent to the EES/EAS service areas. The central ADAE server covers all PLMN area and is used to coordinate or jointly perform analytics with the distributed ADAES. Such analytics services can be provided to consumers at the central DN, like the VAL servers or SEAL services or even at the PLMN side (e.g. NWDAF consuming service experience analytics).

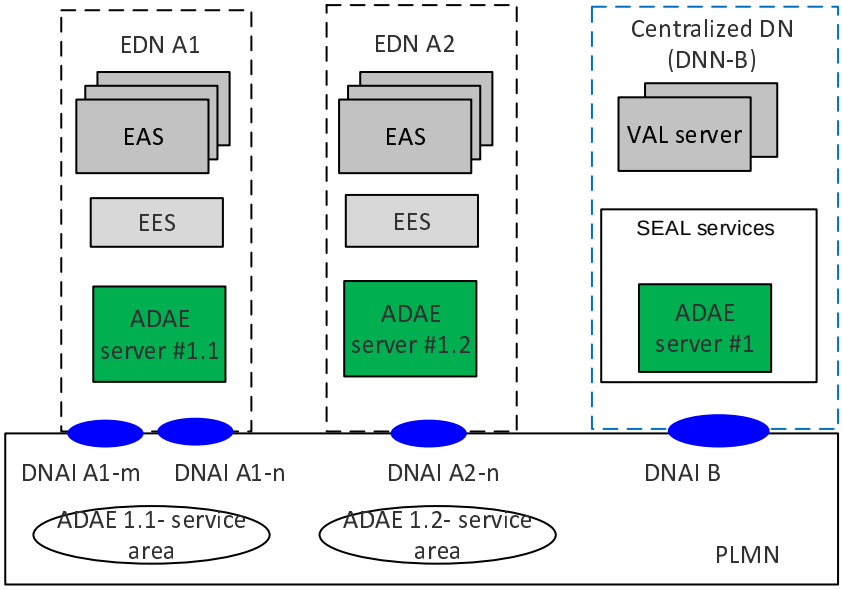

Figure A.4-1: Coordinated deployment of ADAES

Annex B (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2022-10	SA6#51-e					TS skeleton	0.0.0
2022-10	SA6#51-e					Implementation of the following pCRs approved by SA6: S6-222940, S6-222941, S6-222942, S6-222943	0.1.0
2022-11	SA6#52					Implementation of the following pCRs approved by SA6: S6-223235, S6-223237, S6-223455, S6-223456, S6-223494	0.2.0
2023-01	SA6#52-bis-e					Implementation of the following pCRs approved by SA6: S6-230262, S6-230363, S6-230247	0.3.0
2023-03	SA6#53					Implementation of the following pCRs approved by SA6: S6-230939, S6-230847, S6-230848, S6-230849, S6-230850	0.4.0
2023-03	SA#99	SP-230273				Presentation for information at SA#99	1.0.0
2023-04	SA6#54-e					Implementation of the following pCRs approved by SA6: S6-231484, S6-231543, S6-231502, S6-231435, S6-231641, S6-231257, S6-231261, S6-231270.	1.1.0
2023-05	SA6#55					Implementation of the following pCRs approved by SA6: S6-231690, S6-232085, S6-232091.	1.2.0
2023-06	SA#100	SP-230687				Presentation for approval at SA#100	2.0.0
2023-06	SA#100	SP-230687				MCC Editorial update for publication after TSG SA approval (SA#100)	18.0.0
2023-09	SA#101	SP-230996	0001	3	F	Updates to Procedure on Service experience	18.1.0
2023-09	SA#101	SP-230996	0002		F	Adding missing A-ADRF API	18.1.0
2023-12	SA#102	SP-231544	0004	4	F	Extend the edge performance analytics to support transmission quality analytics	18.2.0
2023-12	SA#102	SP-231544	0005	1	F	Updates to Procedure on support for application performance analytics	18.2.0
2023-12	SA#102	SP-231544	0006		F	Updates to Procedure on support for slice-specific application performance analytics	18.2.0
2023-12	SA#102	SP-231544	0007	2	F	Updates to Procedure on support for UE-to-UE application performance analytics	18.2.0
2023-12	SA#102	SP-231544	0008		F	Updates to Procedure on support for location accuracy analytics	18.2.0
2023-12	SA#102	SP-231544	0009		F	Updates to Procedure for supporting service API analytics	18.2.0
2023-12	SA#102	SP-231544	0010		F	Updates to Slice usage pattern analytics	18.2.0
2023-12	SA#102	SP-231544	0011		F	Updates to Procedure for supporting edge load analytics	18.2.0
2023-12	SA#102	SP-231544	0012	3	F	Clarification on parameter of the analytics request	18.2.0
2023-12	SA#102	SP-231544	0014	1	F	Clarification and correction for edge load analytics	18.2.0
2024-03	SA#103	SP-240300	0015		F	Correct edge load analytics	18.3.0
2024-03	SA#103	SP-240300	0016		F	Correct registration	18.3.0
2024-03	SA#103	SP-240300	0020	1	F	Updates to Application Performance Analytics and API	18.3.0
2024-03	SA#103	SP-240300	0021	2	F	Updates to Slice-specific Application Performance Analytics and API	18.3.0
2024-03	SA#103	SP-240300	0022	2	F	Updates to UE-to-UE Application Performance Analytics and API	18.3.0
2024-03	SA#103	SP-240300	0023	1	F	Updates to Location Accuracy Analytics and API	18.3.0
2024-03	SA#103	SP-240300	0024	2	F	Updates to Service API Analytics and API	18.3.0
2024-03	SA#103	SP-240300	0025	2	F	Updates to Slice Usage Pattern Analytics and API	18.3.0
2024-03	SA#103	SP-240300	0026	1	F	Updates to Edge Load Analytics and API	18.3.0
2024-03	SA#103	SP-240320	0019	3	F	Fix the inconsistency of the A-ADRF	19.0.0
2024-06	SA#104	SP-240772	0030	2	B	Edge computing preparation analytics	19.1.0
2024-06	SA#104	SP-240771	0031	2	B	A-ADRF Service for Supporting Data Storage	19.1.0
2024-06	SA#104	SP-240771	0032	1	B	A-DCCF Service for Supporting Data Collection	19.1.0
2024-06	SA#104	SP-240754	0033	1	A	Addition of functional entities and reference points	19.1.0
2024-06	SA#104	SP-240766	0034	1	A	Support for server-to-server performance analytics	19.1.0
2024-09	SA#105	SP-241211	0036	1	A	Alignment with SA4 and CT1	19.2.0
2024-09	SA#105	SP-241220	0037	3	B	Support of Collision Detection Analytics	19.2.0
2024-09	SA#105	SP-241220	0038	3	B	Support of Location-related UE Group Analytics	19.2.0
2024-09	SA#105	SP-241212	0039	3	B	Support of Application Layer AI/ML Member capability Analytics	19.2.0
2024-12	SA#106	SP-241717	0040	5	B	UE RAT connectivity analytics for non terrestrial access	19.3.0
2024-12	SA#106	SP-241715	0043	1	B	Architecture for supporting interactions with AIMLE	19.3.0
2024-12	SA#106	SP-241733	0044	1	B	Support for VAL performance analytics for tethered UEs	19.3.0
2024-12	SA#106	SP-241718	0045	1	B	Updates to Location Accuracy Analytics	19.3.0
2024-12	SA#106	SP-241715	0047	1	B	Push service experience information	19.3.0
2024-12	SA#106	SP-241718	0048	1	B	Updates to application performance analytics	19.3.0
2024-12	SA#106	SP-241718	0049	2	B	Updates to edge load analytics	19.3.0
2024-12	SA#106	SP-241715	0050	1	B	Updates to Application Layer AI/ML Member Capability Analytics	19.3.0
2024-12	SA#106	SP-241720	0051	1	B	Resolves ENs for Collision Detection Analytics	19.3.0
2024-12	SA#106	SP-241718	0053		B	Updates to Slice-specific Application Performance Analytics	19.3.0
2024-12	SA#106	SP-241718	0054		B	Updates to UE-to-UE Application Performance Analytics	19.3.0
2024-12	SA#106	SP-241718	0055	1	B	Updates to Service API Analytics	19.3.0
2024-12	SA#106	SP-241718	0056	1	B	Updates to Slice Usage Pattern Analytics	19.3.0
2024-12	SA#106	SP-241718	0057		F	Updates to Service Experience to Support Application Performance Analytics	19.3.0
2024-12	SA#106	SP-241718	0058		F	Updates to A-ADRF Service on Analytics Storage	19.3.0

2024-12	SA#106	SP-241718	0059		D	Updates to A-DCCF Service on Data Collection	19.3.0
2024-12	SA#106	SP-241715	0060	2	B	Support for DN Energy Analytics	19.3.0
2024-12	SA#106	SP-241715	0061	1	B	ML Model Performance Degradation Detection	19.3.0
2025-06	SA#108	SP-250619	0062		F	Completion of A-ADRF Data Storage Service	19.4.0
2025-06	SA#108	SP-250619	0063	1	F	Adding Security Aspect Description and Reference	19.4.0
2026-03	SA#111	SP-260191	0065		F	Remove ENs on AI/ML Member Capability	19.5.0

History

Version	Date	Status
V19.4.0	January 2026	Publication
V19.5.0	April 2026	Publication