

ETSI TS 123 436 V18.5.0 (2024-10)



**LTE;
5G;**
**Functional architecture and information flows
for Application Data Analytics Enablement Service
(3GPP TS 23.436 version 18.5.0 Release 18)**



Reference

RTS/TSGS-0623436vi50

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

Important notice

The present document can be downloaded from the
ETSI [Search & Browse Standards application](#).

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#).

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

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 Web server (<https://ipr.etsi.org/>).

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™** and **LTE™** 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 under <https://webapp.etsi.org/key/queryform.asp>.

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

Intellectual Property Rights	2
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	7
Introduction	8
1 Scope	9
2 References	9
3 Definitions of terms and abbreviations.....	9
3.1 Terms.....	9
3.2 Abbreviations	10
4 Architectural requirements	10
4.1 General Description.....	10
4.2 General Requirements	10
4.3 ADAE internal architecture requirements	10
4.4 ADAE capability related requirements.....	10
5 Application architecture for ADAES	11
5.1 General	11
5.2 Functional architecture	11
5.2.1 General.....	11
5.2.2 On-network Functional Architecture	11
5.2.3 Off-network Functional Architecture.....	13
5.3 ADAE internal architecture	14
5.4 Functional entities description.....	15
5.4.1 General.....	15
5.4.2 Application Data Analytics Enablement client	15
5.4.3 Application Data Analytics Enablement server	15
5.5 Reference points description	15
5.5.1 General.....	15
5.5.2 ADAE-UU	15
5.5.3 ADAE-PC5	16
5.5.4 ADAE-C	16
5.5.5 ADAE-S.....	16
5.5.4 ADAE-X.....	16
5.5.5 ADAE-Y	16
5.5.6 ADCCF-1.....	16
5.5.7 AADRF-1	16
5.5.8 SEAL-X	16
6 ADAE layer Functional Description	16
6.1 Support for application performance analytics.....	16
6.2 Support for slice-specific application performance analytics.....	17
6.3 Support for UE-to-UE application performance analytics	17
6.4 Support for location accuracy analytics.....	17
6.5 Support for service API analytics.....	17
6.6 Slice usage pattern analytics.....	17
6.7 Support for edge load analytics	17
7 Identities and commonly used values.....	18
7.1 General	18
7.2 ADAE Server ID	18
7.3 ADAE client ID.....	18
7.4 A-ADRF ID.....	18
7.5 A-DCCF ID	18

7.6	Data Producer ID.....	18
7.7	ADAE service area.....	18
7.8	Analytics ID	18
8	Procedures and information flows.....	18
8.1	General	18
8.2	Procedure on support for application performance analytics	19
8.2.1	General.....	19
8.2.2	Procedure on VAL server performance analytics	19
8.2.3	Procedure on VAL session performance analytics	21
8.2.4	Information flows	23
8.2.4.1	General	23
8.2.4.2	VAL performance analytics subscription request	24
8.2.4.3	VAL performance analytics subscription response	24
8.2.4.4	Data collection subscription request	24
8.2.4.5	Data collection subscription response	25
8.2.4.6	Data Notification.....	25
8.2.4.7	Analytics Notification	26
8.2.4.8	Data producer profile	27
8.3	Procedure on support for slice-specific application performance analytics	27
8.3.1	General.....	27
8.3.2	Procedure	27
8.3.3	Information flows	29
8.3.3.1	General	29
8.3.3.2	Slice-specific performance analytics subscription request	29
8.3.3.3	Slice-specific performance analytics subscription response	29
8.3.3.4	Slice-specific performance analytics notification	30
8.4	Procedure on support for UE-to-UE application performance analytics	30
8.4.1	General.....	30
8.4.2	Procedure	30
8.4.3	Information flows	32
8.4.3.1	General	32
8.4.3.2	UE-to-UE session performance analytics subscription request.....	32
8.4.3.3	UE-to-UE session performance analytics subscription response	33
8.4.3.4	UE-to-UE analytics request.....	33
8.4.3.5	UE-to-UE analytics response	33
8.4.3.6	ADAE Analytics Notification	33
8.5	Procedure on support for location accuracy analytics	34
8.5.1	General.....	34
8.5.2	Procedure	34
8.5.3	Information flows	36
8.5.3.1	General	36
8.5.3.2	Location accuracy analytics subscription request	36
8.5.3.3	Location accuracy analytics subscription response	36
8.5.3.4	Location accuracy data request	36
8.5.3.5	Location accuracy data response.....	37
8.5.3.6	Location accuracy analytics notification.....	37
8.6	Procedure for supporting service API analytics	38
8.6.1	General.....	38
8.6.2	Procedure	38
8.6.3	Information flows	39
8.6.3.1	General	39
8.6.3.2	Service API event subscription request.....	39
8.6.3.3	Service API event subscription response	39
8.6.3.4	Historical service API logs request	40
8.6.3.5	Historical service API logs response.....	40
8.6.3.6	Service API analytics notification.....	41
8.7	Slice usage pattern analytics.....	41
8.7.1	General.....	41
8.7.2	Procedure on slice usage pattern analytics.....	41
8.7.3	Procedure on retrieving slice usage statistics data	43
8.7.4	Information flows	43

8.7.4.1	General	43
8.7.4.2	Network slice usage pattern analytics subscription request	43
8.7.4.3	Network slice usage pattern analytics subscription response	44
8.7.4.4	Network slice usage pattern analytics notification	44
8.7.4.5	Network slice data retrieval request	45
8.7.4.6	Network slice data retrieval response	45
8.7.4.7	Slice usage statistics data request	46
8.7.4.8	Slice usage statistics data response	46
8.8	Procedure for supporting edge load analytics	46
8.8.1	General	46
8.8.2	Procedure	46
8.8.2.1	Subscribe-notify model	46
8.8.2.2	Request-response model	48
8.8.3	Information flows	49
8.8.3.1	General	49
8.8.3.2	Edge analytics subscription request	49
8.8.3.3	Edge analytics subscription response	50
8.8.3.4	Edge data collection subscription request	50
8.8.3.5	Edge data collection subscription response	51
8.8.3.6	Data Notification	51
8.8.3.7	Edge analytics Notification	52
8.8.3.8	Get analytics data request	52
8.8.3.9	Get analytics data response	53
8.9	Procedure on Service experience to support application performance analytics	53
8.9.1	General	53
8.9.2	Procedure	54
8.9.2.1	Push service experience information	54
8.9.2.2	Pull service experience information	54
8.9.2.3	Service experience information based on triggers	55
8.9.3	Information flows	55
8.9.3.1	Push service experience information request	55
8.9.3.2	Push service experience information response	56
8.9.3.3	Pull service experience information request	56
8.9.3.4	Pull service experience information response	56
8.9.3.5	Configure service experience report trigger request	57
8.9.3.6	Configure service experience report trigger response	57
9	ADAE layer APIs	57
9.1	General	57
9.2	ADAE server APIs	58
9.2.1	General	58
9.2.2	ADAE server APIs	58
9.2.3	SS_ADAE_VAL_performance_analytics API	58
9.2.3.1	General	58
9.2.3.2	Subscribe	58
9.2.3.3	Notify	58
9.2.4	SS_ADAE_slice_performance_analytics API	59
9.2.4.1	General	59
9.2.4.2	Subscribe	59
9.2.4.3	Notify	59
9.2.5	SS_ADAE_UE-to-UE_performance_analytics API	59
9.2.5.1	General	59
9.2.5.2	Subscribe	59
9.2.5.3	Notify	59
9.2.6	SS_ADAE_location_accuracy_analytics API	60
9.2.6.1	General	60
9.2.6.2	Subscribe	60
9.2.6.3	Notify	60
9.2.7	SS_ADAE_service_API_analytics API	60
9.2.7.1	General	60
9.2.7.2	Subscribe	60
9.2.6.3	Notify	60

9.2.8	SS_ADAE_slice_usage_pattern_analytics API.....	61
9.2.8.1	General.....	61
9.2.8.2	Subscribe.....	61
9.2.8.3	Notify.....	61
9.2.9	SS_ADAE_edge_analytics API.....	61
9.2.9.1	General.....	61
9.2.9.2	Subscribe.....	61
9.2.9.3	Notify.....	61
9.2.9.4	Get.....	62
9.2.10	SS_ADAE_slice_usage_stats.....	62
9.2.10.1	General.....	62
9.2.10.2	Get.....	62
9.3	A-ADRF APIs.....	62
9.3.1	General.....	62
9.3.2	A-ADRF APIs.....	62
9.3.3	SS_AADRF_Data_Collection API.....	63
9.3.3.1	General.....	63
9.3.3.2	Subscribe.....	63
9.3.3.3	Notify.....	63
9.3.4	SS_AADRF_Historical_serviceAPI_logs API.....	63
9.3.4.1	General.....	63
9.3.4.2	Get.....	63
9.3.5	SS_AADRF_NetworkSlice_data API.....	64
9.3.5.1	General.....	64
9.3.5.2	Get.....	64
9.3.6	SS_AADRF_EdgeData_Collection API.....	64
9.3.6.1	General.....	64
9.3.6.2	Subscribe.....	64
9.3.6.3	Notify.....	64
9.3.7	SS_AADRF_Location_Accuracy API.....	65
9.3.7.1	General.....	65
9.3.7.2	Get.....	65
Annex A (informative): Deployment scenarios.....		66
A.1	General.....	66
A.2	Deployment model #1: Cloud-deployed ADAES.....	66
A.3	Deployment model #2 Edge-deployed ADAES.....	66
A.4	Deployment model #3: Coordinated ADAES deployment.....	67
Annex B (informative): Change history.....		69
History	70

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 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".
- [15] 3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

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.

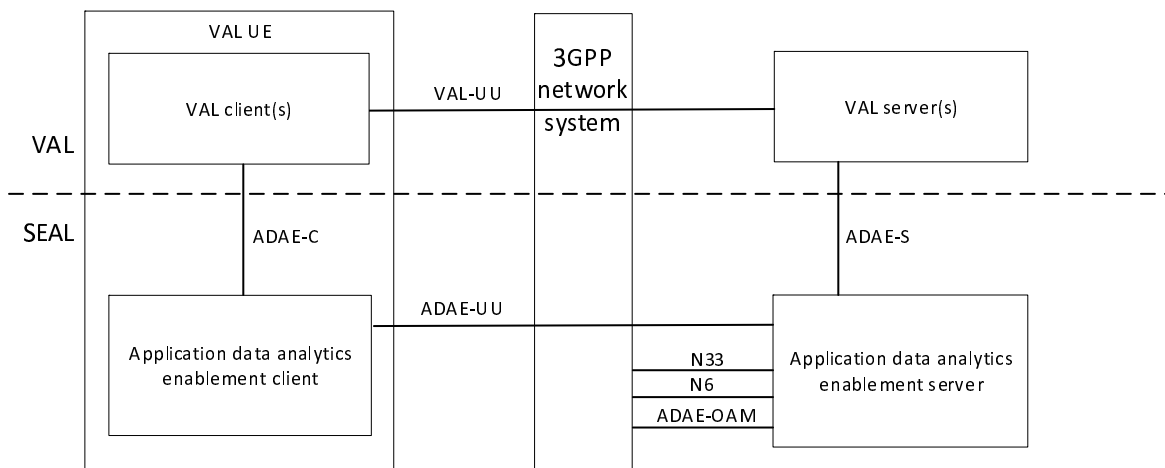


Figure 5.2.2-1: Architecture for application data analytics enablement – reference points representation

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.

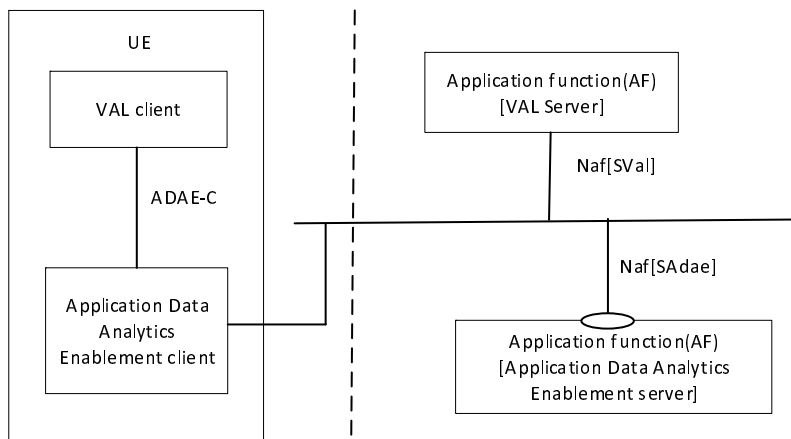


Figure 5.2.2-2: Architecture for application data analytics enablement – Service based representation

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].

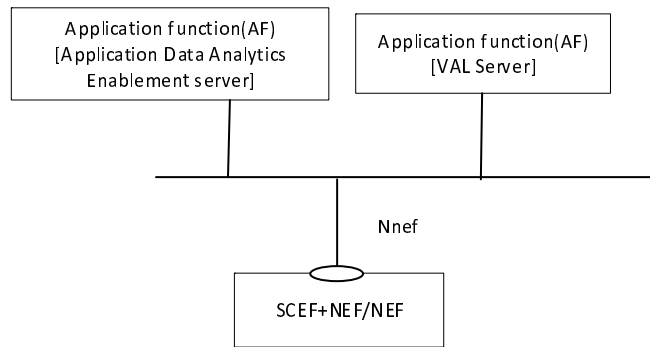


Figure 5.2.2-3: Architecture for application data analytics enablement utilizing the 5GS network services based on the 5GS SBA – Service based representation

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

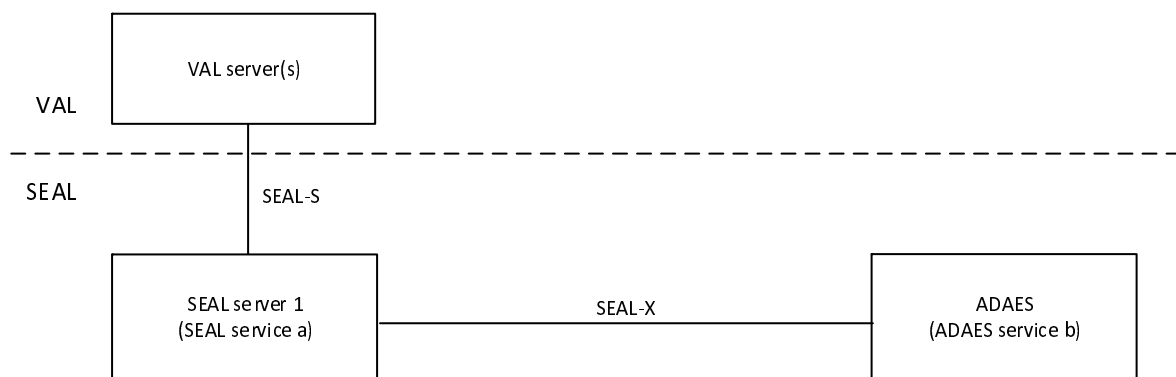


Figure 5.2.2-4: Inter-service communication between ADAES server and other SEAL server

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.

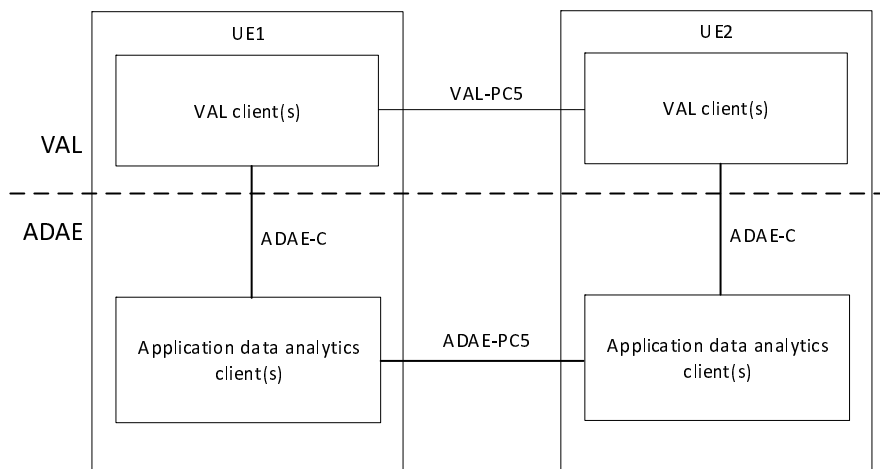


Figure 5.2.3-1: Generic off-network functional model

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].

5.3 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.

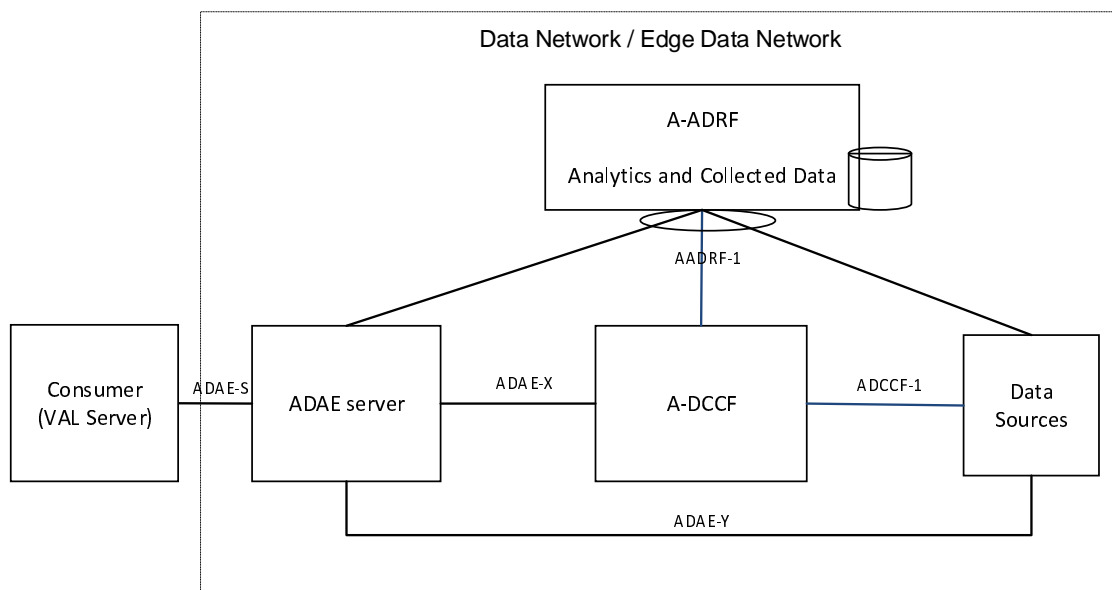


Figure 5.3-1: ADAE internal functional architecture

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 functionalities 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;

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 [14] 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 [15].

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].

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.

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.

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 is 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.

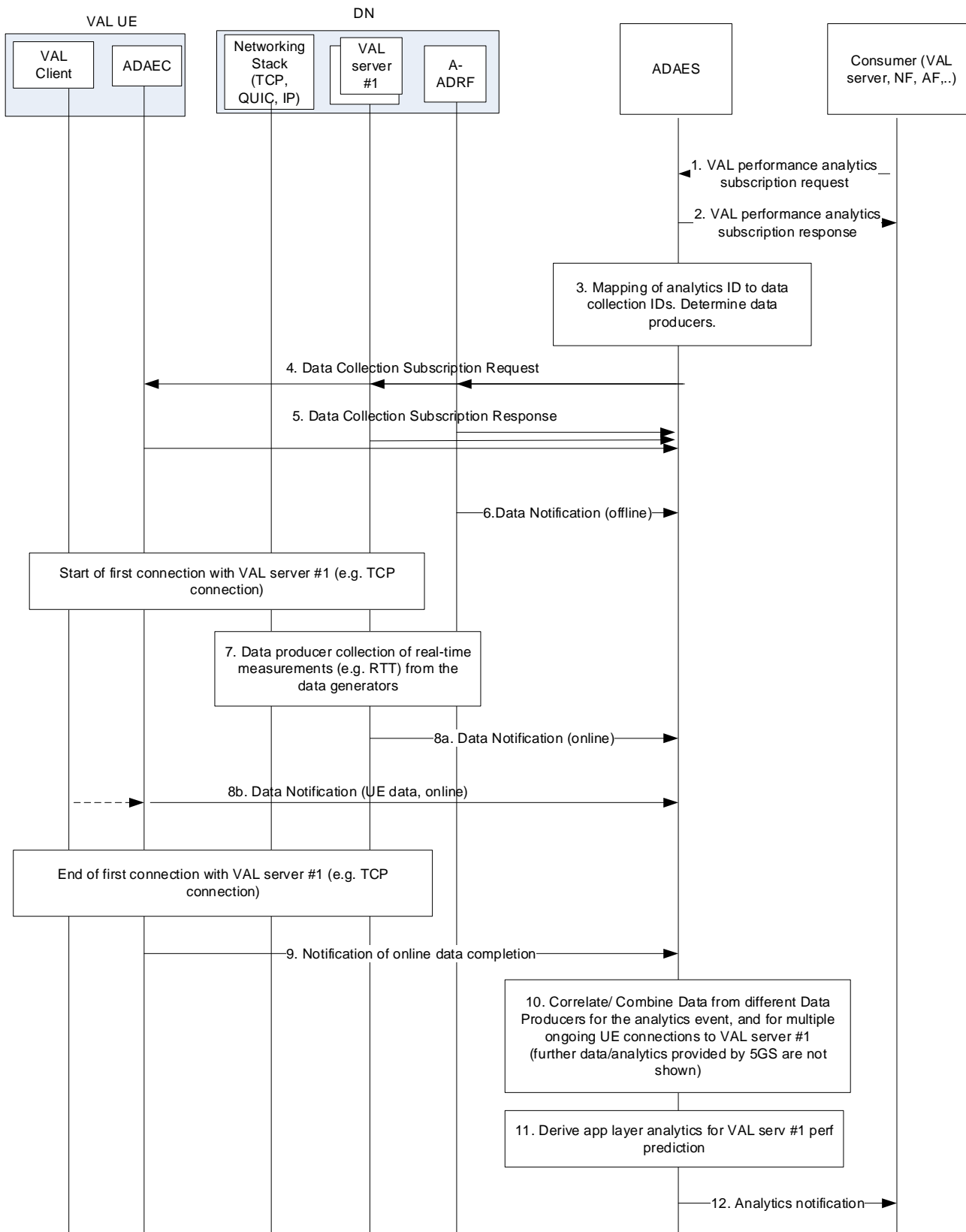


Figure 8.2.2-1: ADAES support for VAL server performance analytics

1. The consumer of the ADAES analytics service sends a VAL performance analytics subscription request to ADAES.
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, whether offline/online analytics were used.

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.

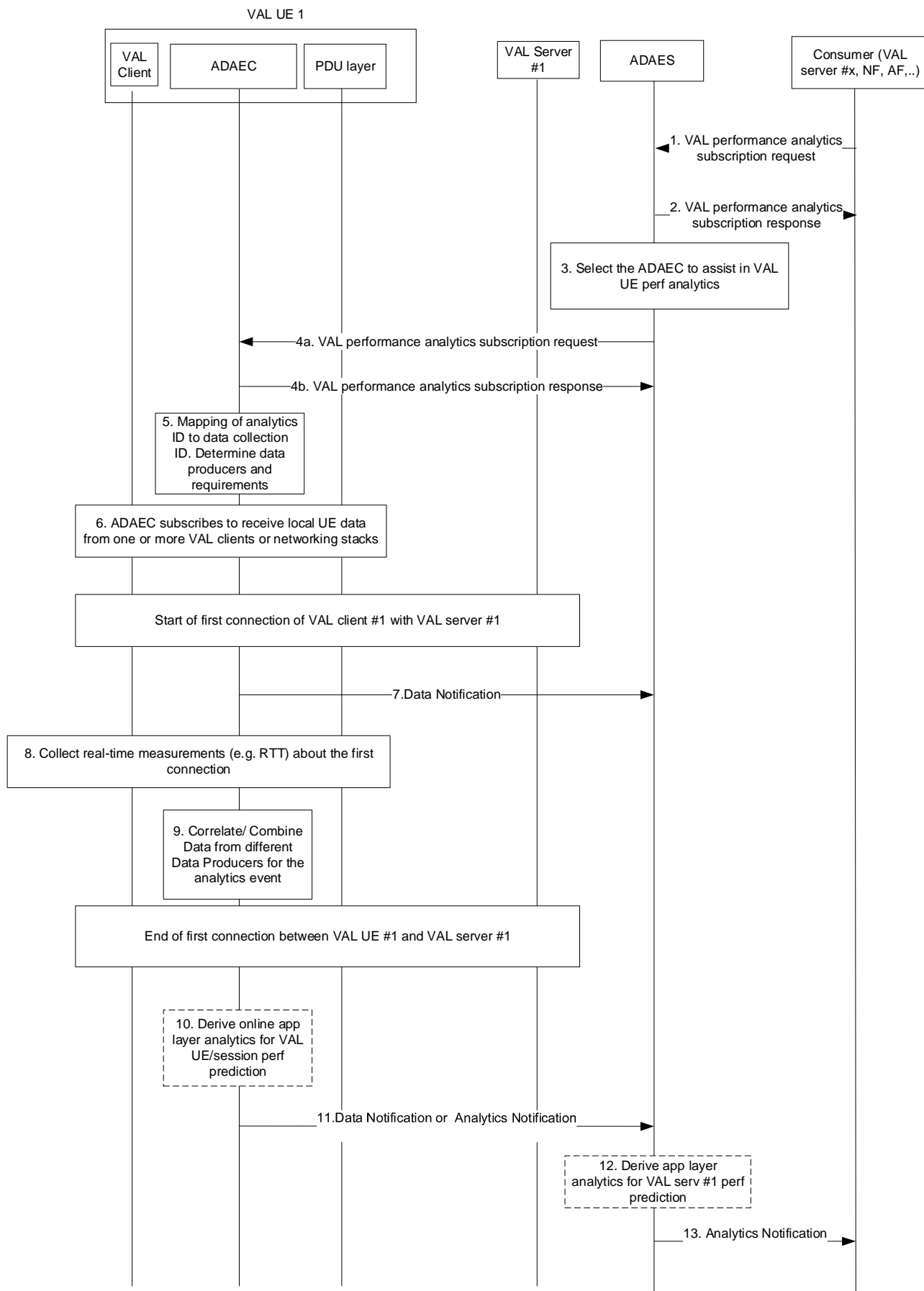


Figure 8.2.3-1: ADAES support for VAL session performance analytics

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 UE perf prediction", 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 threshold or event).
- 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 performance for a given area and time horizon, including also the confidence level, whether offline/online analytics were used.

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 VAL server / Consumer 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 apply.
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 8.2.2).
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.

8.2.4.3 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/VAL server 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).

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	O	The VAL UE(s) identifiers and IP address(es) for which the data collection subscription apply
Target VAL server ID	O	This identifier shows the target VAL server for which the data collection subscription applies (for procedure in 8.2.2)
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

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) 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	M (NOTE)	The VAL UE(s) identifiers 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 (for procedure in 8.2.2)
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 (e.g. RTT deviation) based on subscription
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 VAL server / Consumer.

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 predictive or statistical parameter, which can be: <ul style="list-style-type: none"> - A VAL server predicted or expected performance change or sustainability - A VAL session predicted or expected performance change of sustainability
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: These information elements shall be provided for the predictive analytics.		

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.

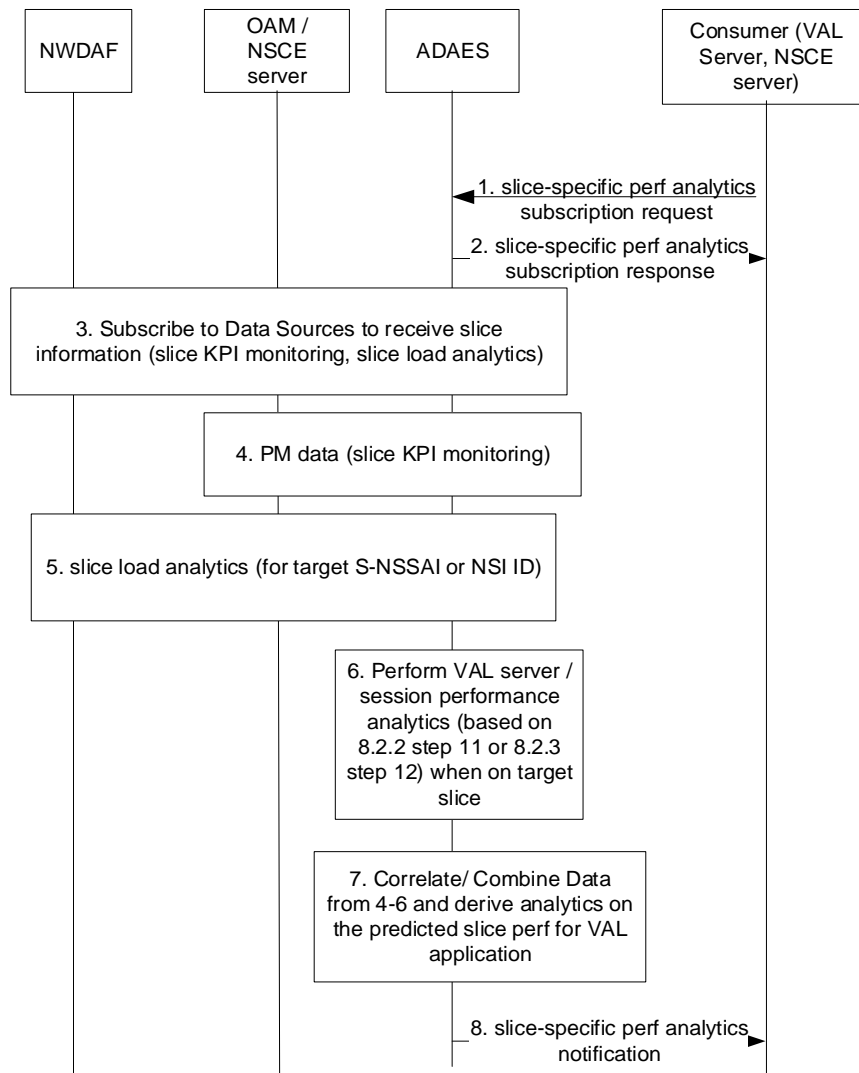


Figure 8.3.2-1: ADAES support for slice-related performance analytics

1. The consumer of the ADAES analytics service sends a subscription request to ADAES and provides the analytics event ID e.g. "slice perf prediction", the target S-NSSAI, DNN, NSI ID, the time validity of the request, the required confidence level, whether offline and/or online analytics are needed, 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	M	The identifier of the target slice or slice instance, 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 8.2.2).
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.
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.
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, which can be for a target slice or slice instance the: <ul style="list-style-type: none"> - A VAL server predicted or expected performance change or sustainability - A VAL session predicted or expected performance change of sustainability
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.

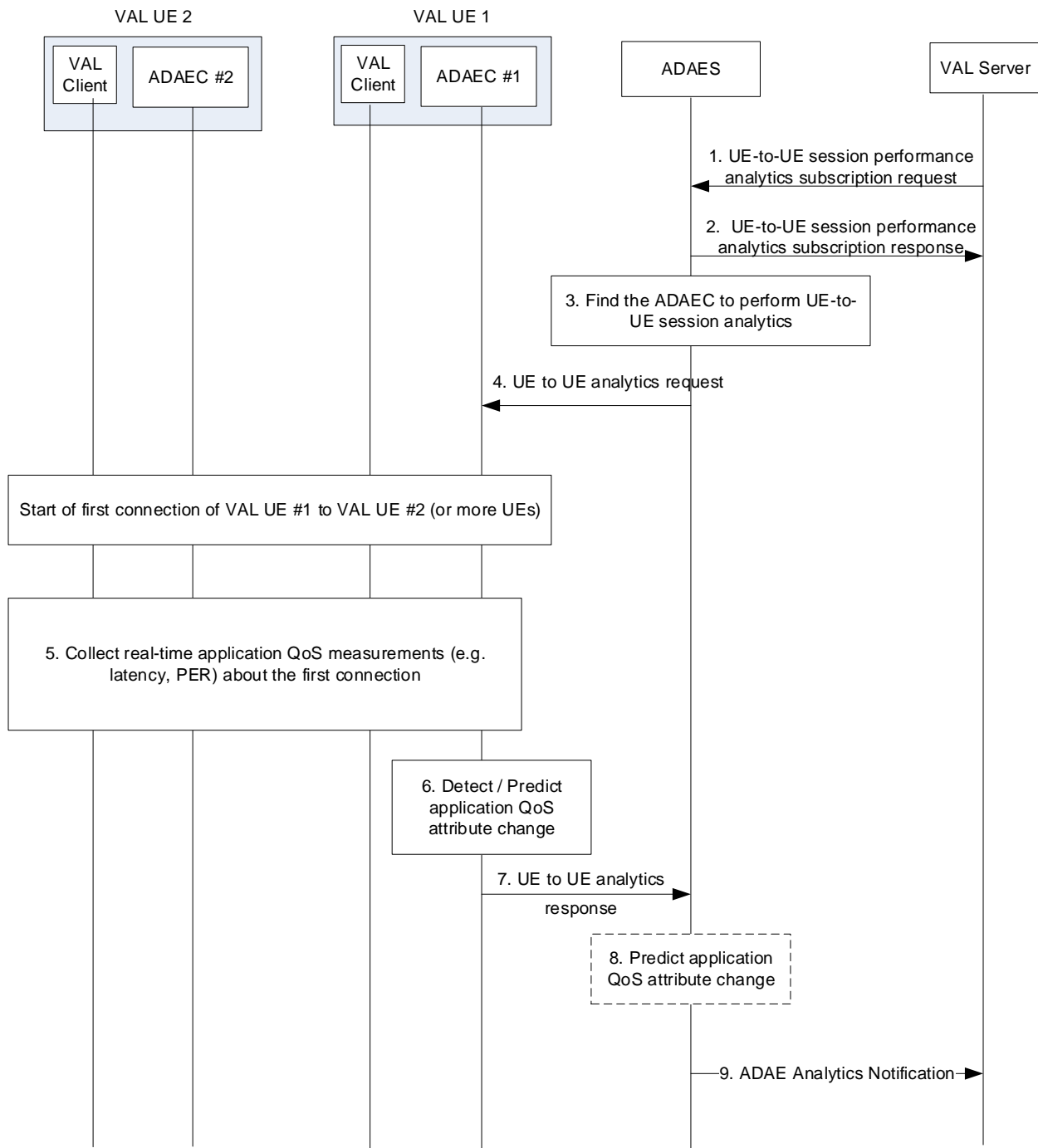


Figure 8.4.2-1: ADAES support for UE-to-UE application performance analytics

1. The consumer of the ADAES analytics service sends a subscription request to ADAES and provides the analytics event ID e.g. "VAL UE to UE session prediction", the target VAL UE ID or group of UE IDs, the VAL session / 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 UEs 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 event ID and the configuration of the reporting required (e.g., periodic, based on threshold(s) or event). 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.
List of VAL UE IDs and addresses	M	The VAL UEs for which the analytics subscription applies.
VAL service ID	O	The VAL service for which the subscription applies.
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 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), the reporting periodicity in case of periodic, and reporting thresholds.

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 session analytics').
List of VAL UE IDs and addresses	M	The VAL UE(s) identifiers 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), 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 subscription 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.
List of VAL UE IDs and addresses	M	The VAL UE(s) identifiers 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 predictive or statistical parameter, which can be: <ul style="list-style-type: none"> - A VAL UE to UE session predicted or expected performance change - A VAL UE to UE session performance sustainability over a given time horizon/area
Confidence level	O	For predictive analytics, the achieved confidence level can be provided.

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.

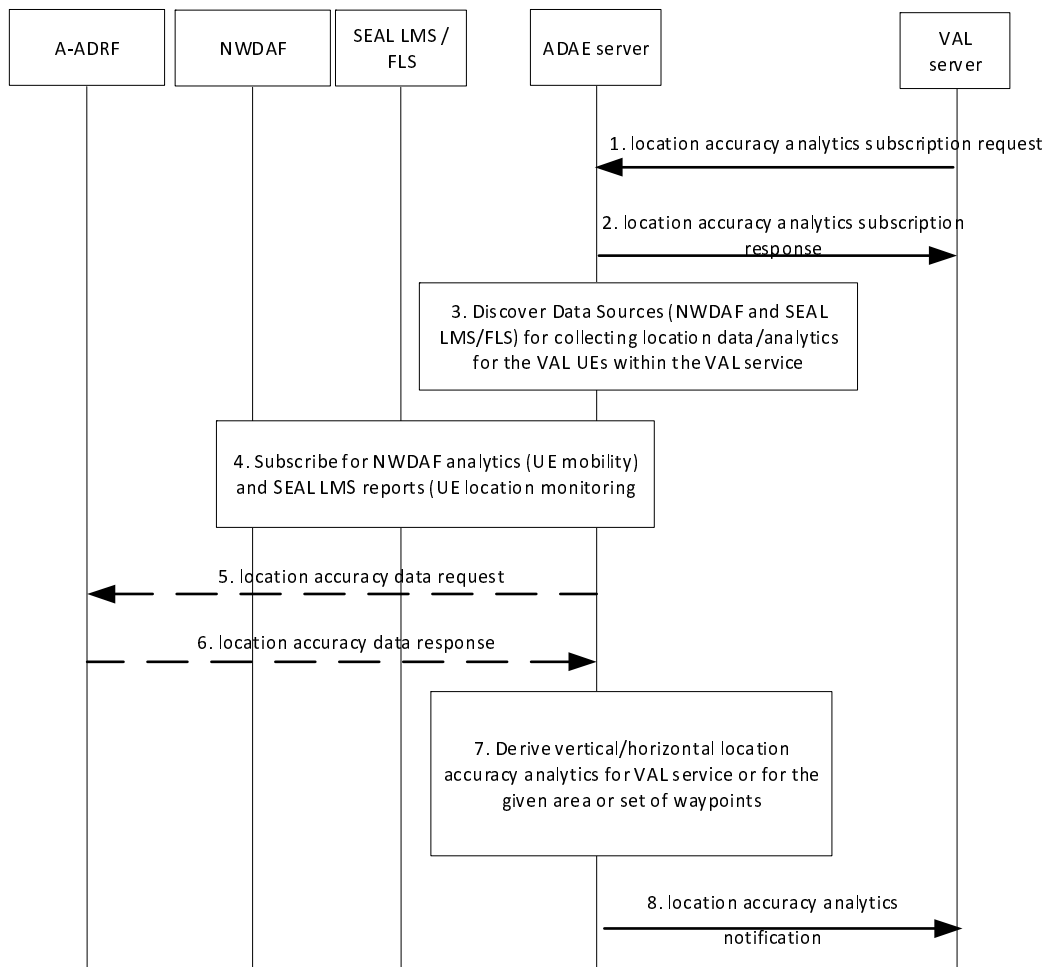


Figure 8.5.2-1: Location accuracy analytics procedure

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.
Analytics Output	M	The predictive or statistical parameter, which can be: <ul style="list-style-type: none"> - A predicted or expected location accuracy change (downgrade or upgrade) for a particular VAL service or UEs - the location accuracy sustainability for a VAL service or UE/group of UEs over a given time horizon/area
Confidence level	O	For predictive analytics, the achieved confidence level can be provided.

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

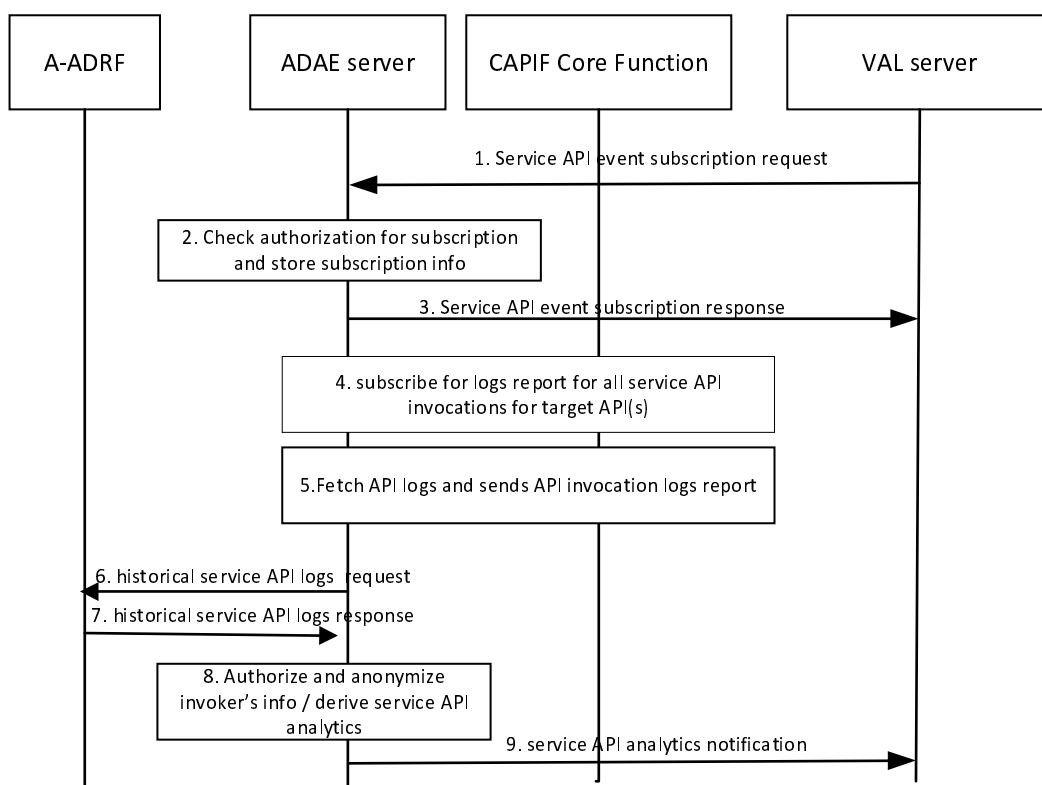


Figure 8.6.2 -1: Service API analytics procedure

1. The VAL server sends a service API event subscription request to the ADAE server to receive analytics for one or more service APIs.
2. Upon receiving the event 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 and horizon	O	Time validity of the subscription request and time horizon for the predictions.
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.

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. the frequency of reporting (periodic), the reporting periodicity in case of periodic, and 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
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 8.6.3.5-1 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
Consumer ID	M	The information to determine the identity of the subscribing entity (consumer)
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.

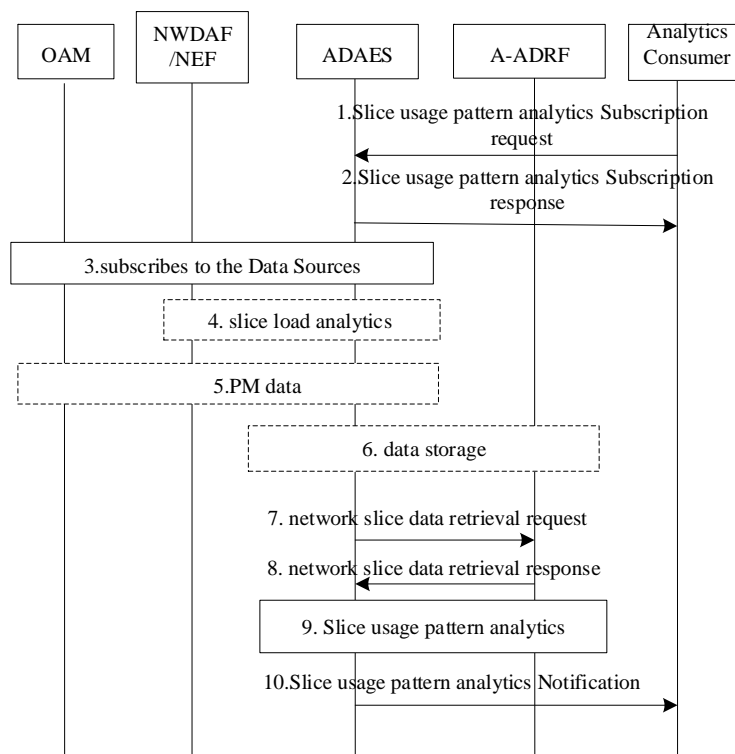


Figure 8.7.2-1: Procedure for network slice usage pattern analytics

1. The analytics consumer of the ADAES sends a 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, whether offline and/or online analytic are needed etc. Optionally, the slice requirement could also be provided.
2. The ADAES sends a 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, 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 network 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.

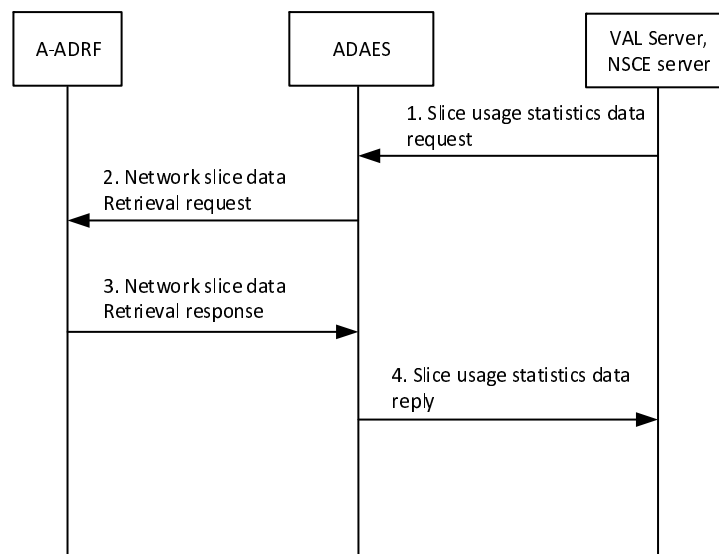


Figure 8.7.3-1: Retrieving of slice usage statistics data procedure

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 reply 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 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 (for procedure in 8.2.2)
>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.

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.
>Analytics ID	M	The identifier of the analytics event
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	M	The identifier of the analytics event.
> Slice usage pattern analytics	M	Analytics of network slice usage pattern (e.g., periodicity of slice usage peak).

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	O	The VAL UE(s) identifiers and IP address(es) for which the data collection subscription apply
Target VAL server ID	O	This identifier shows 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
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 and address	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
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 ADAES 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.
> 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 ADAES 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, for which the data collection is needed.
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.
>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.

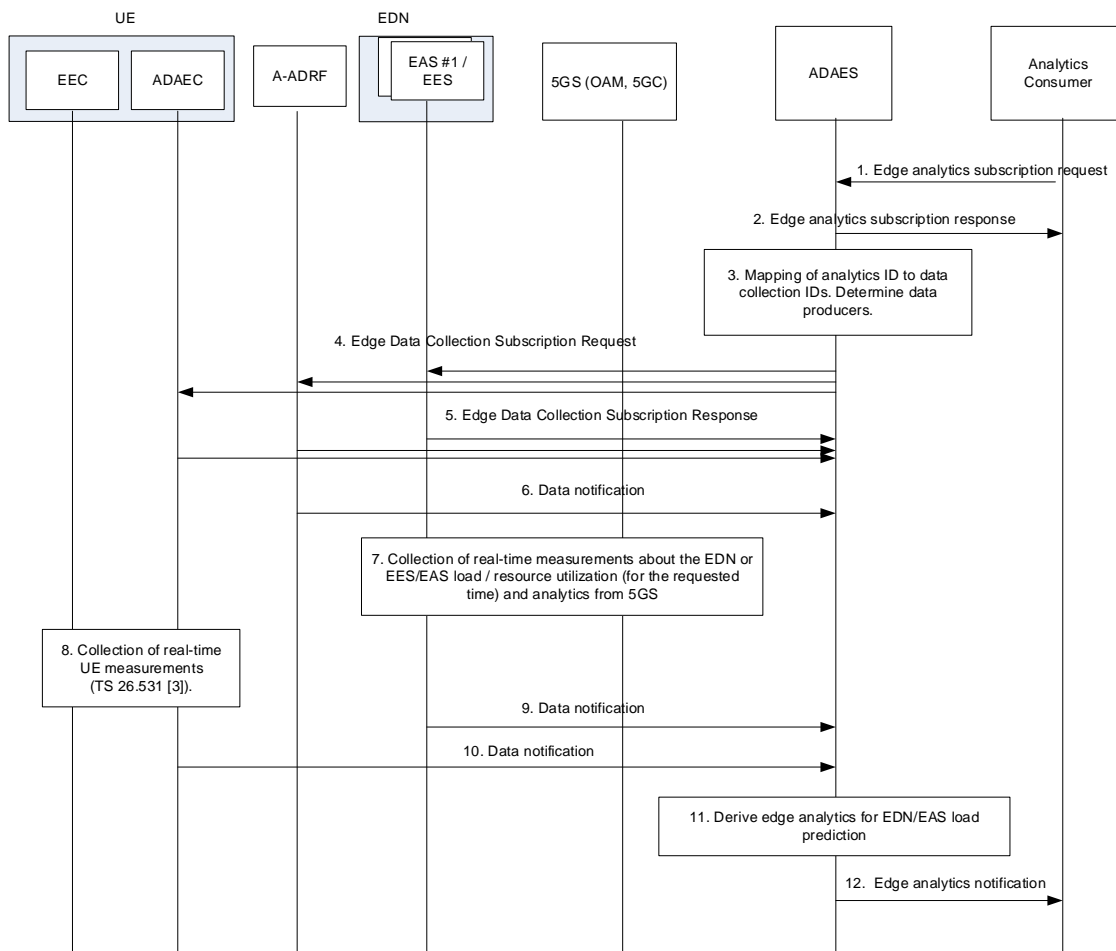


Figure 8.8.2.1-1: ADAES support for edge analytics

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.

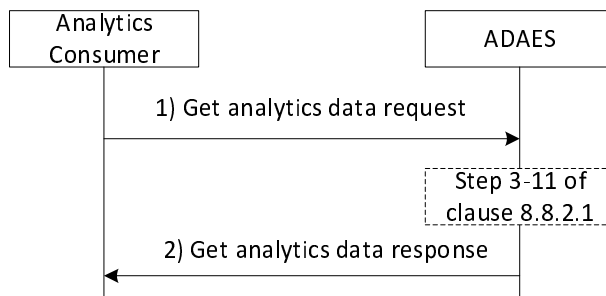


Figure 8.8.2.2-1: ADAES support for edge analytics

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 performance 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 DNAs 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 predictive or statistical parameter, which can be stats or prediction related to the edge performance/load for the edge platform or EES/EAS for a given area/time and based on the event type.
Confidence level	O	For predictive analytics, the achieved confidence level can be provided.

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 performance 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 edge analytics subscription response from the ADAE server to the consumer.

Table 8.8.3.9-1: Edge analytics subscription 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 predictive or statistical parameter, which can be stats or prediction related to the edge performance/load for the edge platform or EES/EAS for a given area/time and based on the event type.
Confidence level	O	For predictive analytics, the achieved confidence level can be provided.

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. In this release, such indirect reporting procedure is implementation specific.

Editor's note: If the data collection mechanisms, necessary to meet the requirements to specify solution#5 of the TR 23.700-36, are not supported by 3GPP TS 26.531 [3], such mechanisms will be defined in this version of the specification based on the conclusions in TR 23.700-36.

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 VAL client or any other trigger conditions, the ADAE client sends the service experience report about a VAL server to the ADAE server using the mechanism defined in 3GPP TS 26.531 [3]. 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].

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 other UEs. Use the service experience information report from other UEs, to determine/predict analytics.

- If most of the UE side entities report a 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 a 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 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.

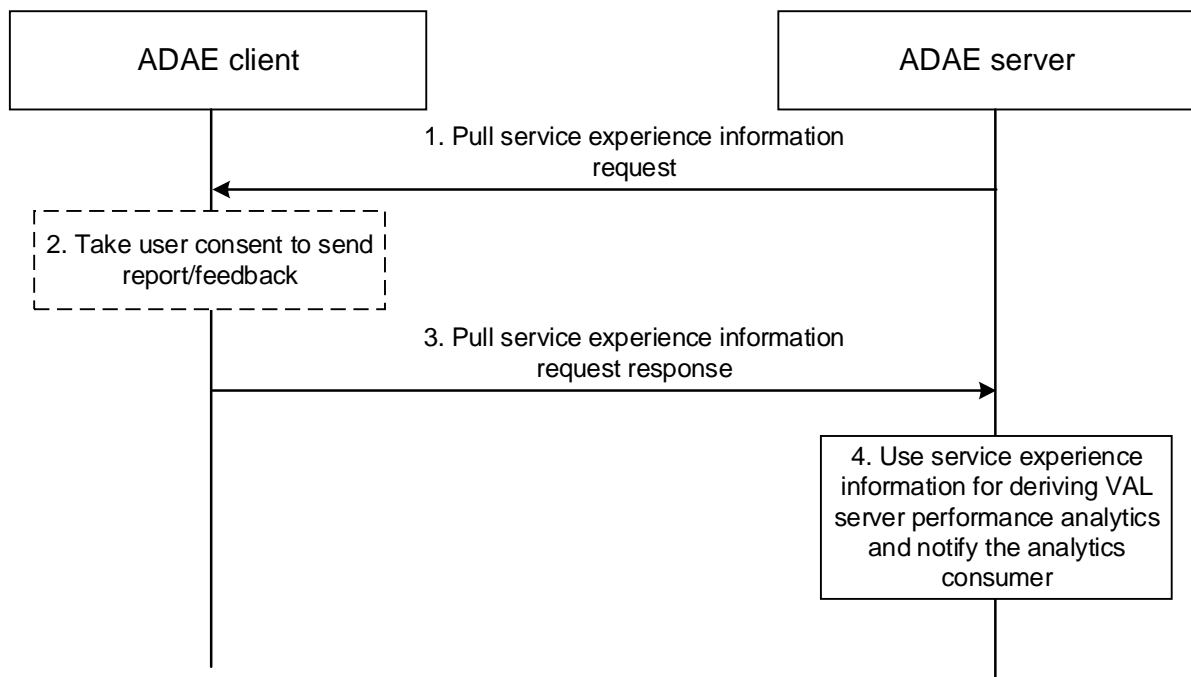


Figure 8.9.2.2-1: Pull service experience information from UE

1. The ADAE server sends Pull service experience request to the ADAE client. The request contains identity 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 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 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	Identity of the VAL UE.
VAL service ID	O	Identity of the VAL service.
VAL Server Id	M	Identify 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 Identity	M	Identity of the VAL server for which the service experience information is requested.
VAL service ID	O	Identity of the VAL service.

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 whether the report is available or not
VAL UE ID	M	Identity of the VAL UE.
VAL service ID (NOTE)	O	Identity of the VAL service.
VAL Server Id	M	Identify 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	Identify the list of VAL servers for which the service experience report is requested List of VAL server specific criteria.
> VAL Server Id	M	Identity 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 ASM 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 server to the ADAE client.

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.

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_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

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.

9.3 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	

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.

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.

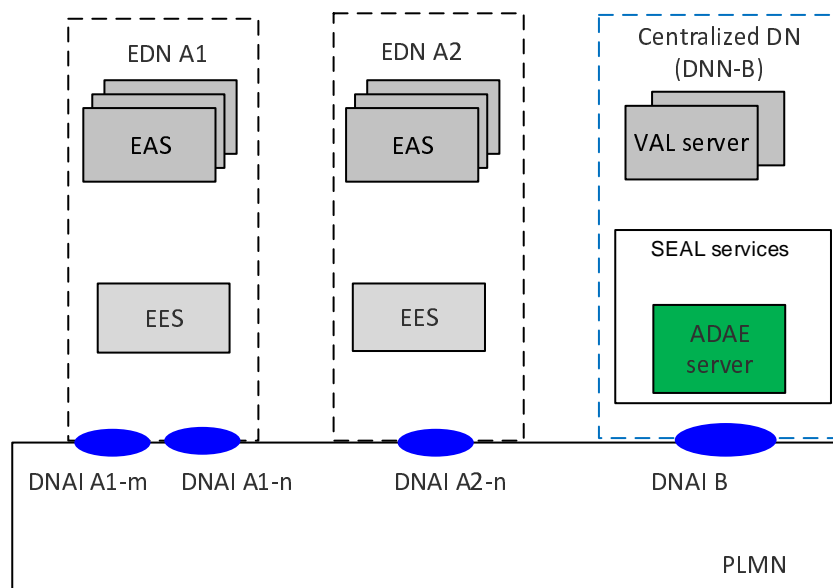


Figure A.2-1: Cloud deployed ADAES

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.

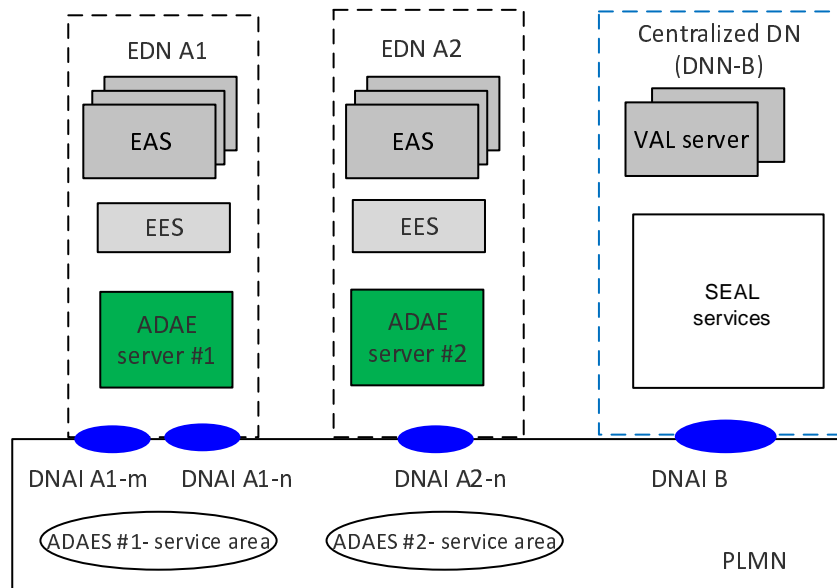


Figure A.3-1: Edge deployed ADAES

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).

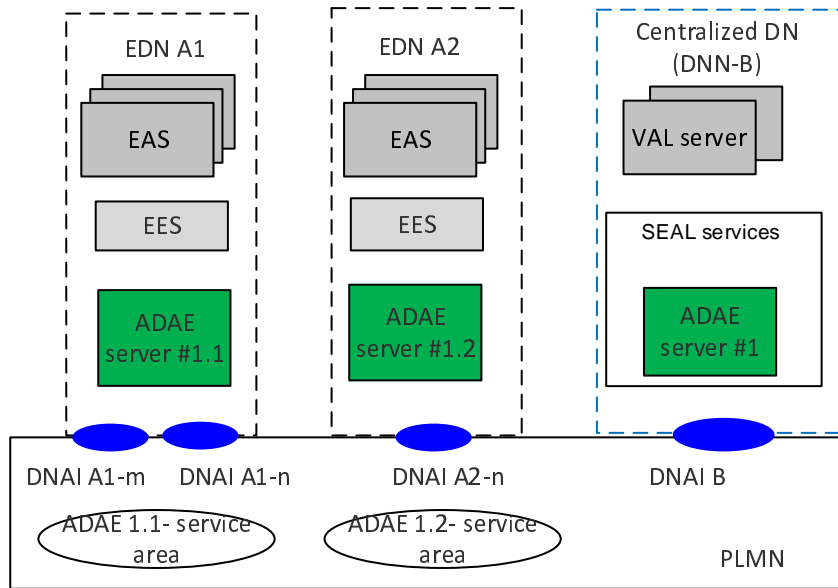


Figure A.4-1: Coordinated deployment of ADAES

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
2024-06	SA#104	SP-240300	0029	2	F	Addition of functional entities and reference points	18.4.0
2024-09	SA#105	SP-241211	0035	1	F	Alignment with SA4 and CT1	18.5.0

History

Document history		
V18.3.0	April 2024	Publication
V18.4.0	July 2024	Publication
V18.5.0	October 2024	Publication