

ETSI TS 123 558 V17.6.0 (2023-01)



5G; Architecture for enabling Edge Applications (3GPP TS 23.558 version 17.6.0 Release 17)



ReferenceRTS/TSGS-0623558vh60

Keywords5G

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:

<http://www.etsi.org/standards-search>

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 at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

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 2023.
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 <http://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.....	12
Introduction	12
1 Scope	13
2 References	13
3 Definitions of terms, symbols and abbreviations	14
3.1 Terms.....	14
3.2 Symbols.....	15
3.3 Abbreviations	15
4 Overview	15
4.1 General	15
4.2 Service provisioning.....	16
4.3 Registration	16
4.4 EAS discovery.....	16
4.5 Capability exposure to EAS	16
4.6 Support for service continuity	16
4.7 Security	17
4.8 Dynamic EAS instantiation triggering	17
4.9 Charging.....	17
5 Architectural requirements	17
5.1 General	17
5.2 Architectural requirements	17
5.2.1 General requirements.....	17
5.2.1.1 General	17
5.2.1.2 Requirements	17
5.2.2 Edge configuration data	17
5.2.2.1 General	17
5.2.2.2 Requirements	17
5.2.3 Registration.....	18
5.2.3.1 General	18
5.2.3.2 EEC registration.....	18
5.2.3.3 EAS registration.....	18
5.2.3.4 EES registration	18
5.2.4 EAS discovery	18
5.2.4.1 General	18
5.2.4.2 Requirements	18
5.2.5 Capability exposure to EASs	19
5.2.5.1 General	19
5.2.5.2 Requirements	19
5.2.6 Security	19
5.2.6.1 General	19
5.2.6.2 Requirements	19
5.2.7 Subscription service.....	19
5.2.7.1 General	19
5.2.7.2 Requirements	19
5.2.8 Traffic management.....	20
5.2.8.1 General	20
5.2.8.2 Requirements	20
5.2.9 Lifecycle management.....	20
5.2.9.1 General	20

5.2.9.2	Requirements	20
5.2.10	Edge application KPIs	20
5.2.10.1	General	20
5.2.10.2	Requirements	20
5.2.11	Service continuity	20
5.2.11.1	General	20
5.2.11.2	Requirements	21
6	Application layer architecture	21
6.1	General	21
6.2	Architecture	21
6.3	Functional entities	23
6.3.1	General	23
6.3.2	Edge Enabler Server (EES)	23
6.3.3	Edge Enabler Client (EEC)	24
6.3.4	Edge Configuration Server (ECS)	24
6.3.5	Application Client (AC)	24
6.3.6	Edge Application Server (EAS)	24
6.4	Service-based interfaces	25
6.5	Reference Points	25
6.5.1	General	25
6.5.2	EDGE-1	25
6.5.3	EDGE-2	25
6.5.4	EDGE-3	26
6.5.5	EDGE-4	26
6.5.6	EDGE-5	26
6.5.7	EDGE-6	26
6.5.8	EDGE-7	26
6.5.9	EDGE-8	26
6.5.10	EDGE-9	27
6.6	Cardinality rules	28
6.6.1	General	28
6.6.2	Functional Entity Cardinality	28
6.6.2.1	General	28
6.6.2.2	AC	28
6.6.2.3	EEC	28
6.6.2.4	ECS	28
6.6.2.5	EES	28
6.6.2.6	EAS	28
6.6.3	Reference Point Cardinality	29
6.6.3.1	General	29
6.6.3.2	EDGE-1 (Between EEC and EES)	29
6.6.3.3	EDGE-3 (Between EAS and EES)	29
6.6.3.4	EDGE-4 (Between EEC and ECS)	29
6.6.3.5	EDGE-5 (Between AC and EEC)	29
6.6.3.6	EDGE-6 (Between EES and ECS)	29
6.6.3.7	EDGE-9 (Between EES and EES)	29
6.7	Capability exposure for enabling edge applications	29
6.7.1	General	29
6.7.2	APIs provided by the Edge Enabler Layer	30
7	Identities and commonly used values	31
7.1	General	31
7.2	Identities	31
7.2.1	General	31
7.2.2	Edge Enabler Client ID (EECID)	31
7.2.3	Edge Enabler Server ID (EESID)	31
7.2.4	Edge Application Server ID (EASID)	32
7.2.5	Application Client ID (ACID)	32
7.2.6	UE ID	32
7.2.7	UE Group ID	32
7.2.8	EEC Context ID	32

7.3	Commonly used values	32
7.3.1	General.....	32
7.3.2	UE location	32
7.3.3	Service areas	33
7.3.3.1	General	33
7.3.3.2	Topological Service Area.....	33
7.3.3.3	Geographical Service Area.....	33
7.3.3.4	EDN service area	33
7.3.3.5	EES Service Area.....	33
7.3.3.6	EAS service area	34
8	Procedures and information flows.....	34
8.1	General	34
8.2	Common Information Elements	34
8.2.1	General.....	34
8.2.2	AC Profile.....	34
8.2.3	AC Service KPIs.....	34
8.2.4	EAS Profile	35
8.2.5	EAS Service KPIs.....	35
8.2.6	EES Profile	36
8.2.7	Topological Service Area	36
8.2.8	EEC Context	37
8.2.9	Geographical Service Area	37
8.3	ECS Discovery and Service provisioning	38
8.3.1	General.....	38
8.3.2	ECS Discovery.....	40
8.3.2.1	General	40
8.3.2.2	Procedures	40
8.3.2.2.1	General	40
8.3.2.3	Information flows.....	40
8.3.2.3.1	General	40
8.3.2.4	APIs.....	40
8.3.2.4.1	General	40
8.3.3	Service provisioning	41
8.3.3.1	General	41
8.3.3.2	Procedures	41
8.3.3.2.1	General	41
8.3.3.2.2	Request-response model	41
8.3.3.2.3	Subscribe-notify model	42
8.3.3.2.3.1	General.....	42
8.3.3.2.3.2	Subscribe.....	42
8.3.3.2.3.3	Notify.....	44
8.3.3.2.3.4	Subscription update.....	44
8.3.3.2.3.5	Unsubscribe	45
8.3.3.3	Information flows.....	46
8.3.3.3.1	General	46
8.3.3.3.2	Service provisioning request	46
8.3.3.3.3	Service provisioning response	47
8.3.3.3.4	Service provisioning subscription request	48
8.3.3.3.5	Service provisioning subscription response.....	49
8.3.3.3.6	Service provisioning notification.....	49
8.3.3.3.7	Service provisioning subscription update request	49
8.3.3.3.8	Service provisioning subscription update response	50
8.3.3.3.9	Service provisioning unsubscribe request.....	50
8.3.3.3.10	Service provisioning unsubscribe response	50
8.3.3.4	APIs.....	51
8.3.3.4.1	General	51
8.3.3.4.2	Eecs_ServiceProvisioning_Request operation	51
8.3.3.4.3	Eecs_ServiceProvisioning_Subscribe operation.....	51
8.3.3.4.4	Eecs_ServiceProvisioning_Notify operation.....	51
8.3.3.4.5	Eecs_ServiceProvisioning_UpdateSubscription operation.....	51
8.3.3.4.6	Eecs_ServiceProvisioning_Unsubscribe operation	52

8.4	Registration	52
8.4.1	General.....	52
8.4.2	EEC Registration	52
8.4.2.1	General	52
8.4.2.2	Procedures	52
8.4.2.2.1	General	52
8.4.2.2.2	EEC registration	52
8.4.2.2.3	EEC registration update.....	54
8.4.2.2.4	EEC de-registration	54
8.4.2.3	Information flows.....	55
8.4.2.3.1	General	55
8.4.2.3.2	EEC registration request.....	55
8.4.2.3.3	EEC registration response	56
8.4.2.3.4	EEC registration update request	56
8.4.2.3.5	EEC registration update response.....	57
8.4.2.3.6	EEC de-registration request.....	57
8.4.2.3.7	EEC de-registration response	57
8.4.2.4	APIs.....	58
8.4.2.4.1	General	58
8.4.2.4.2	Ees_EECRegistration_Request operation.....	58
8.4.2.4.3	Ees_EECRegistration_Update operation	58
8.4.2.4.4	Ees_EECRegistration_Deregister operation	58
8.4.3	EAS Registration	59
8.4.3.1	General	59
8.4.3.2	Procedures	59
8.4.3.2.1	General	59
8.4.3.2.2	EAS registration	59
8.4.3.2.3	EAS registration update.....	60
8.4.3.2.4	EAS de-registration	60
8.4.3.3	Information flows.....	61
8.4.3.3.1	General	61
8.4.3.3.2	EAS registration request.....	61
8.4.3.3.3	EAS registration response	61
8.4.3.3.4	EAS registration update request	62
8.4.3.3.5	EAS registration update response.....	62
8.4.3.3.6	EAS de-registration request.....	62
8.4.3.3.7	EAS de-registration response	63
8.4.3.4	APIs.....	63
8.4.3.4.1	General	63
8.4.3.4.2	Ees_EASRegistration_Request operation.....	63
8.4.3.4.3	Ees_EASRegistration_Update operation	63
8.4.3.4.4	Ees_EASRegistration_Deregister operation	63
8.4.4	EES Registration.....	64
8.4.4.1	General	64
8.4.4.2	Procedures	64
8.4.4.2.1	General	64
8.4.4.2.2	EES registration.....	64
8.4.4.2.3	EES registration update	64
8.4.4.2.4	EES de-registration.....	65
8.4.4.3	Information elements	66
8.4.4.3.1	General	66
8.4.4.3.2	EES registration request	66
8.4.4.3.3	EES registration response	66
8.4.4.3.4	EES registration update request.....	66
8.4.4.3.5	EES registration update response	66
8.4.4.3.6	EES de-registration request	67
8.4.4.3.7	EES de-registration response.....	67
8.4.4.4	APIs.....	67
8.4.4.4.1	General	67
8.4.4.4.2	Eecs_EESRegistration_Request operation	67
8.4.4.4.3	Eecs_EESRegistration_Update operation	68
8.4.4.4.4	Eecs_EESRegistration_Deregister operation	68

8.5	EAS discovery	68
8.5.1	General	68
8.5.2	Procedures	69
8.5.2.1	General	69
8.5.2.2	Request-response model	69
8.5.2.3	Subscribe-notify model	70
8.5.2.3.1	General	70
8.5.2.3.2	Subscribe	71
8.5.2.3.3	Notify	72
8.5.2.3.4	Subscription update	73
8.5.2.3.5	Unsubscribe	73
8.5.3	Information flows	74
8.5.3.1	General	74
8.5.3.2	EAS discovery request	74
8.5.3.3	EAS discovery response	76
8.5.3.4	EAS discovery subscription request	76
8.5.3.5	EAS discovery subscription response	77
8.5.3.6	EAS discovery notification	77
8.5.3.7	EAS discovery subscription update request	78
8.5.3.8	EAS discovery subscription update response	78
8.5.3.9	EAS discovery unsubscribe request	78
8.5.3.10	EAS discovery unsubscribe response	78
8.5.4	APIs	79
8.5.4.1	General	79
8.5.4.2	Eees_EASDiscovery_Request operation	79
8.5.4.3	Eees_EASDiscovery_Subscribe operation	79
8.5.4.4	Eees_EASDiscovery_Notify operation	79
8.5.4.5	Eees_EASDiscovery_UpdateSubscription operation	80
8.5.4.6	Eees_EASDiscovery_Unsubscribe operation	80
8.6	EES capability exposure to EAS	80
8.6.1	General	80
8.6.2	UE location API	80
8.6.2.1	General	80
8.6.2.2	Procedures	80
8.6.2.2.1	General	80
8.6.2.2.2	Request-response model	80
8.6.2.2.3	Subscribe-notify model	81
8.6.2.2.3.1	General	81
8.6.2.2.3.2	Subscribe	81
8.6.2.2.3.3	Notify	82
8.6.2.2.3.4	Subscription update	83
8.6.2.2.3.5	Unsubscribe	84
8.6.2.3	Information flows	84
8.6.2.3.1	General	84
8.6.2.3.2	UE location request	85
8.6.2.3.3	UE location response	85
8.6.2.3.4	UE location subscribe request	85
8.6.2.3.5	UE location subscribe response	85
8.6.2.3.6	UE location notification	86
8.6.2.3.7	UE location subscription update request	86
8.6.2.3.8	UE location subscription update response	86
8.6.2.3.9	UE location unsubscribe request	86
8.6.2.3.10	UE location unsubscribe response	87
8.6.2.4	APIs	87
8.6.2.4.1	General	87
8.6.2.4.2	Eees_UELocation_Get operation	87
8.6.2.4.3	Eees_UELocation_Subscribe operation	87
8.6.2.4.4	Eees_UELocation_Notify operation	87
8.6.2.4.5	Eees_UELocation_UpdateSubscription operation	88
8.6.2.4.6	Eees_UELocation_Unsubscribe operation	88
8.6.3	ACR management events	88
8.6.3.1	General	88

8.6.3.2	Procedures	89
8.6.3.2.1	General	89
8.6.3.2.2	Subscribe	89
8.6.3.2.3	Notify	90
8.6.3.2.4	Subscription update	91
8.6.3.2.5	Unsubscribe	92
8.6.3.3	Information flows.....	93
8.6.3.3.1	General	93
8.6.3.3.2	ACR management event subscribe request	93
8.6.3.3.3	ACR management event subscribe response	93
8.6.3.3.4	ACR management event notification.....	94
8.6.3.3.5	ACR management event subscription update request	94
8.6.3.3.6	ACR management event subscription update response	95
8.6.3.3.7	ACR management event unsubscribe request	95
8.6.3.3.8	ACR management event unsubscribe response	95
8.6.3.4	APIs.....	96
8.6.3.4.1	General	96
8.6.3.4.2	Eees_ACRManagementEvent_Subscribe operation.....	96
8.6.3.4.3	Eees_ACRManagementEvent_Notify operation.....	96
8.6.3.4.4	Eees_ACRManagementEvent_UpdateSubscription operation.....	96
8.6.3.4.5	Eees_ACRManagementEvent_Unsubscribe operation	97
8.6.4	AC information exposure API	97
8.6.4.1	General	97
8.6.4.2	Procedures	97
8.6.4.2.1	General	97
8.6.4.2.2	Subscribe	97
8.6.4.2.3	Notify	98
8.6.4.2.4	Subscription update	98
8.6.4.2.5	Unsubscribe	99
8.6.4.3	Information flows.....	99
8.6.4.3.1	General	99
8.6.4.3.2	AC information subscription request.....	99
8.6.4.3.3	AC information subscription response	100
8.6.4.3.4	AC information notification	100
8.6.4.3.5	AC information subscription update request	101
8.6.4.3.6	AC information subscription update response.....	101
8.6.4.3.7	AC information unsubscribe request	101
8.6.4.3.8	AC information unsubscribe response.....	101
8.6.4.4	APIs.....	102
8.6.4.4.1	General	102
8.6.4.4.2	Eees_AppClientInformation_Subscribe operation	102
8.6.4.4.3	Eees_AppClientInformation_Notify operation.....	102
8.6.4.4.4	Eees_AppClientInformation_UpdateSubscription operation	102
8.6.4.4.5	Eees_AppClientInformation_Unsubscribe operation	102
8.6.5	UE Identifier API.....	103
8.6.5.1	General	103
8.6.5.2	Procedure	103
8.6.5.3	Information flows.....	103
8.6.5.3.1	General	103
8.6.5.3.2	UE Identifier API request	104
8.6.5.3.3	UE Identifier API response.....	104
8.6.5.4	APIs.....	104
8.6.5.4.1	General	104
8.6.5.4.2	Eees_UEIdentifier_Get operation.....	104
8.6.6	Session with QoS API.....	104
8.6.6.1	General	104
8.6.6.2	Procedures	105
8.6.6.2.1	General	105
8.6.6.2.2	Create a session	105
8.6.6.2.3	Update a session	106
8.6.6.2.4	Revoke a session.....	107
8.6.6.2.5	Notify	107

8.6.6.3	Information flows.....	108
8.6.6.3.1	General	108
8.6.6.3.2	Session with QoS create request.....	108
8.6.6.3.3	Session with QoS create response	109
8.6.6.3.4	Session with QoS update request.....	109
8.6.6.3.5	Session with QoS update response	110
8.6.6.3.6	Session with QoS revoke request	110
8.6.6.3.7	Session with QoS revoke response	110
8.6.6.3.8	Session with QoS event notification.....	111
8.6.6.4	APIs.....	111
8.6.6.4.1	General	111
8.6.6.4.2	Eees_SessionWithQoS_Create operation.....	111
8.6.6.4.3	Eees_SessionWithQoS_Update operation.....	112
8.6.6.4.4	Eees_SessionWithQoS_Revoke operation.....	112
8.6.6.4.5	Eees_SessionWithQoS_Notify operation.....	112
8.7	Network capability exposure to EAS	112
8.7.1	General.....	112
8.7.2	Direct network capability exposure	112
8.7.3	Network capability exposure via EES	112
8.8	Service continuity	113
8.8.1	General.....	113
8.8.1.1	High level overview	113
8.8.1.2	ACR with service continuity planning	115
8.8.1.3	Unused contexts handling during ACR including service continuity planning.....	115
8.8.2	Scenarios.....	115
8.8.2.1	General	115
8.8.2.2	Initiation by EEC using regular EAS Discovery	116
8.8.2.3	EEC executed ACR via S-EES	119
8.8.2.4	S-EAS decided ACR scenario.....	120
8.8.2.5	S-EES executed ACR.....	122
8.8.2.6	EEC executed ACR via T-EES	125
8.8.3	Procedures.....	127
8.8.3.1	General	127
8.8.3.2	Discover T-EAS	127
8.8.3.3	Retrieve T-EES procedure	128
8.8.3.4	ACR launching procedure.....	128
8.8.3.5	ACR information subscription	130
8.8.3.5.1	General	130
8.8.3.5.2	Subscribe	130
8.8.3.5.3	Notify	131
8.8.3.5.4	Subscription update	131
8.8.3.5.5	Unsubscribe	132
8.8.3.6	EELManagedACR procedure	133
8.8.3.6.1	General	133
8.8.3.6.2	Procedure.....	133
8.8.3.6.2.1	General.....	133
8.8.3.6.2.2	ACR request.....	133
8.8.3.6.2.3	ACT status subscription.....	134
8.8.3.6.2.4	ACT status notification	134
8.8.3.7	Selected T-EAS declaration	134
8.8.3.8	ACR status update procedure.....	135
8.8.4	Information flows	136
8.8.4.1	General	136
8.8.4.2	EAS discovery request.....	136
8.8.4.3	EAS discovery response.....	136
8.8.4.4	ACR request.....	136
8.8.4.5	ACR response	137
8.8.4.6	Retrieve EES request.....	138
8.8.4.7	Retrieve EES response	138
8.8.4.8	ACR information subscription request.....	138
8.8.4.9	ACR information subscription response	138
8.8.4.10	ACR information notification	139

8.8.4.11	ACR information subscription update request	139
8.8.4.12	ACR information subscription update response	139
8.8.4.13	ACR information unsubscribe request	140
8.8.4.14	ACR information unsubscribe response	140
8.8.4.15	EELManagedACR service request	140
8.8.4.16	EELManagedACR service response	141
8.8.4.17	Selected target EAS declaration request	141
8.8.4.18	Selected target EAS declaration response	141
8.8.4.19	ACR status update request	141
8.8.4.20	ACR status update response	142
8.8.4.21	ACT status subscription request	142
8.8.4.22	ACT status subscription response	142
8.8.4.23	ACT status notification	143
8.8.5	APIs	143
8.8.5.1	General	143
8.8.5.2	Eees_TargetEASDiscovery API	143
8.8.5.2.1	General	143
8.8.5.2.2	Eees_TargetEASDiscovery_Request operation	143
8.8.5.3	Eees_AppContextRelocation API	144
8.8.5.3.1	General	144
8.8.5.3.2	Eees_AppContextRelocation_Request operation	144
8.8.5.4	Eecs_TargetEESDiscovery API	144
8.8.5.4.1	General	144
8.8.5.4.2	Eecs_TargetEESDiscovery_Request operation	144
8.8.5.5	Eees_ACREvents API	144
8.8.5.5.1	General	144
8.8.5.5.2	Eees_ACREvents_Subscribe operation	144
8.8.5.5.3	Eees_ACREvents_Notify operation	144
8.8.5.5.4	Eees_ACREvents_UpdateSubscription operation	145
8.8.5.5.5	Eees_ACREvents_Unsubscribe operation	145
8.8.5.6	Eees_EELManagedACR API	145
8.8.5.6.1	General	145
8.8.5.6.2	Eees_EELManagedACR_Request operation	145
8.8.5.6.3	Eees_EELManagedACR_Subscribe operation	145
8.8.5.6.4	Eees_EELManagedACR_Notify operation	145
8.8.5.7	Eees_SelectedTargetEAS API	146
8.8.5.7.1	General	146
8.8.5.7.2	Eees_SelectedTargetEAS_Declare operation	146
8.8.5.8	Eees_ACRStatusUpdate API	146
8.8.5.8.1	General	146
8.8.5.8.2	Eees_ACRStatusUpdate_Request operation	146
8.9	EEC Context and EEC Context relocation	146
8.9.1	General	146
8.9.1.1	EEC Context handling at EEC registration	147
8.9.1.2	EEC Context handling at EEC registration update	147
8.9.1.3	EEC Context handling at EEC de-registration	147
8.9.1.4	EEC Context handling at Application Context Relocation	147
8.9.1.5	Other EEC Context handling	147
8.9.2	Procedures	148
8.9.2.1	General	148
8.9.2.2	EEC Context Pull relocation	148
8.9.2.3	EEC Context Push relocation	149
8.9.3	Information flows	149
8.9.3.1	General	149
8.9.3.2	EEC Context Pull request	149
8.9.3.3	EEC Context Pull response	150
8.9.3.4	EEC Context Push request	150
8.9.3.5	EEC Context Push response	150
8.9.4	APIs	151
8.9.4.1	General	151
8.9.4.2	Eees_EECContextPull API	151
8.9.4.2.1	General	151

8.9.4.2.2	Eees_EECContextPull_Request operation	151
8.9.4.3	Eees_EECContextPush API	151
8.9.4.3.1	General	151
8.9.4.3.2	Eees_EECContextPush_Request operation	151
8.10	Utilizing 3GPP core network capabilities	151
8.10.1	General	151
8.10.2	Capabilities utilized by ECS	152
8.10.3	Capabilities utilized by EES	152
8.11	EEC Authentication/Authorization	152
8.11.1	General	152
8.12	Dynamic EAS instantiation triggering	152
8.12.1	General	152
8.13	Charging	153
Annex A (Informative): Deployment models		154
A.1	General	154
A.2	Deployment models for different DN implementations	154
A.2.1	General	154
A.2.2	Option 1. Use of non-dedicated DN	154
A.2.3	Option 2. Use of Edge-dedicated DN	155
A.2.4	Option 3. Use of LADN	155
A.3	ECS deployments in relation to the UE	156
A.3.1	General	156
A.3.2	UE (EEC) served by a single ECS	156
A.3.3	UE (EECs) served by multiple ECSs	156
A.4	Deployment of EES in relation with SEAL services and Application Enabler Services	156
A.4.1	General	156
A.4.2	Deployment of SEAL services	158
A.4.3	Deployment of Application Enabler services	158
A.5	Deployments in relation with CAPIF	158
A.5.1	General	158
A.5.2	Distributed CAPIF	158
A.5.3	Centralized CAPIF	160
Annex B (Informative): Involved entities and relationships		162
B.1	General	162
Annex C (Informative): Relationship with ETSI MEC architecture		163
C.1	General	163
C.2	Relationship between EDGEAPP and ETSI MEC architectures	163
Annex D (Informative): Relationship with GSMA OPG		165
D.1	General	165
D.2	Relationship between EDGEAPP architecture and GSMA OPG reference architecture	165
Annex E (informative): Change history		166
History		170

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.

Introduction

Edge Computing is a network architecture concept that enables cloud computing capabilities and service environments, which are deployed close to the UE. It promises several benefits such as lower latency, higher bandwidth, reduced backhaul traffic and prospects for new services compared to the cloud environments. This technical specification provides application layer architecture and related procedures for enabling edge applications over 3GPP networks.

1 Scope

The present document specifies the application layer architecture, procedures and information flows necessary for enabling edge applications over 3GPP networks. It includes architectural requirements for enabling edge applications, application layer architecture fulfilling the architecture requirements and procedures to enable the deployment of edge applications.

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 23.501: "System architecture for the 5G System (5GS); Stage 2".
- [3] 3GPP TS 23.502: "Procedure for the 5G System (5GS); Stage 2".
- [4] 3GPP TS 29.522: "5G System; Network Exposure Function Northbound APIs; Stage 3".
- [5] 3GPP TS 29.122: "T8 reference point for northbound Application Programming Interfaces (APIs)".
- [6] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2".
- [7] 3GPP TS 23.271: "Functional stage 2 description of Location Services (LCS)".
- [8] 3GPP TS 36.305: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN".
- [9] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".
- [10] 3GPP TS 38.305: "NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN".
- [11] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".
- [12] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".
- [13] 3GPP TS 23.434: "Service enabler architecture layer for verticals; Functional architecture and information flows; Stage 2".
- [14] 3GPP TS 23.286: "Application layer support for Vehicle-to-Everything (V2X) services; Functional architecture and information flows".
- [15] ETSI ISG MEC ETSI GS MEC 003 V2.1.1 (2019-01), "Multi-access Edge Computing (MEC); Framework and Reference Architecture"
- [16] Void
- [17] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

- [18] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".
- [19] GSMA Whitepaper OPG.01: "Operator Platform: Telco Edge Proposal", <https://www.gsma.com/futurenetworks/wp-content/uploads/2020/10/GSMA-Operator-Platform-Proposal-Oct-2020.pdf>
- [20] 3GPP TS 23.548: "5G System Enhancements for Edge Computing".
- [21] 3GPP TS 23.032: "Universal Geographical Area Description (GAD)".
- [22] 3GPP TS 28.538: "Management and orchestration; Edge Computing Management".
- [23] 3GPP TS 33.558: "Security aspects of enhancement of support for enabling edge applications".
- [24] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".
- [25] 3GPP TS 32.257: "Telecommunication management; Charging management; Edge computing domain charging".

3 Definitions of terms, symbols 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].

Application Context: A set of data about the Application Client that resides in the Edge Application Server.

Application Context Relocation: Refers to the end-to-end service continuity procedure described in clause 8.8.

Application Context Transfer: Refers to the transfer of the Application Context between the source Edge Application Server and the target Edge Application Server, which is a part of the service continuity procedure described in clause 8.8.

Application Server: Application software resident in the cloud performing the server function.

Edge Computing: A concept, as described in 3GPP TS 23.501 [2], that enables operator and 3rd party services to be hosted close to the UE's access point of attachment, to achieve an efficient service delivery through the reduced end-to-end latency and load on the transport network.

Edge Computing Service Provider: A mobile network operator or a 3rd party service provider offering Edge Computing service.

Edge Data Network: A local Data Network that supports the architecture for enabling edge applications.

EEC Context: A set of data about the Edge Enabler Client that resides in the Edge Enabler Server.

Edge Enabler Layer: Refers to the overall functionality provided by the entities such as Edge Enabler Client, Edge Enabler Server and Edge Configuration Server, in support of applications as per the architecture defined in clause 6.

Edge Hosting Environment: An environment providing support required for Edge Application Server's execution.

3.2 Symbols

None.

3.3 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].

AC	Application Client
ACID	Application Client Identification
ACR	Application Context Relocation
ACT	Application Context Transfer
AF	Application Function
ASP	Application Service Provider
DN	Data Network
DNAI	Data Network Access Identifier
DNN	Data Network Name
EAS	Edge Application Server
EASID	Edge Application Server Identification
ECS	Edge Configuration Server
ECSP	Edge Computing Service Provider
EDN	Edge Data Network
EEC	Edge Enabler Client
EECID	Edge Enabler Client Identification
EEL	Edge Enabler layer
EES	Edge Enabler Server
EESID	Edge Enabler Server Identification
FQDN	Fully Qualified Domain Name
GPSI	Generic Public Subscription Identifier
GSM	Global System for Mobile Communications
GSMA	GSM Association
LADN	Local Area Data Network
NEF	Network Exposure Function
OP	Operator Platform
OPG	Operator Platform Group
S-EAS	Source Edge Application Server
S-EES	Source Edge Enabler Server
SCEF	Service Capability Exposure Function
SSID	Service Set Identifier
T-EAS	Target Edge Application Server
T-EES	Target Edge Enabler Server
TAI	Tracking Area Identity

4 Overview

4.1 General

For edge computing, it is essential that the ACs are able to locate and connect with the most suitable application server available in the EDN, depending on the needs of the application. The edge enabler layer exposes APIs to support such capabilities.

The edge computing capabilities supported by 3GPP are illustrated in the figure 4.1-1.

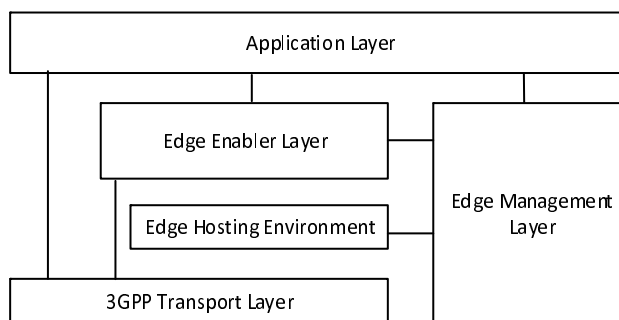


Figure 4.1-1: Overview of 3GPP edge computing

The application layer is a consumer of 3GPP specified edge computing capabilities. The 3GPP edge computing capabilities are typically organized as follows:

- Edge enabler layer, specified in this specification;
- Edge hosting environment, details of which are outside the scope of 3GPP;
- 3GPP transport layer, specified in 3GPP TS 23.401 [11] and 3GPP TS 23.501 [2]; and
- Edge management layer, specified in 3GPP TS 28.538 [22].

Following clauses provide an overview of the features of edge enabler layer.

4.2 Service provisioning

Service provisioning procedures supply the information required by the UE to access the edge services. The procedure takes UE's location, service requirements, service preferences and connectivity information into account to provide the required configuration. Service provisioning procedures are specified in clause 8.3.

4.3 Registration

Registration procedures specified in clause 8.4, allow entities (e.g. UE and Application Server) in the edge enabler layer to provide information about itself to other entities of the edge enabler layer.

4.4 EAS discovery

EAS discovery procedures enable the UE to obtain information about suitable EASs of interest (specified as discovery filters) in the EDN. EAS discovery procedures are specified in clause 8.5.

4.5 Capability exposure to EAS

The edge enabler layer exposes services towards the EASs. The exposed capabilities include the services of the Edge Enabler Layer and the re-exposed and enhanced services of the 3GPP core network. The capabilities exposed by the edge enabler layer are specified in clause 8.6 and the 3GPP network capability exposure is specified in clause 8.7. Other application layer capabilities like application enabler services and SEAL services may be exposed via edge enabler layer as per CAPIF as illustrated in Annex A.4.

4.6 Support for service continuity

When a UE moves to a new location, different EASs can be more suitable for serving the UE. Such transitions can result from a non-mobility event also, requiring support from the edge enabler layer to maintain the continuity of the service. Support for service continuity provides several features for minimizing the application layer service interruption by replacing the S-EAS connected to the AC in the UE, with a T-EAS. Support for service continuity is further specified in clause 8.8.

4.7 Security

The edge enabler layer supports secure communication amongst the enabler layer entities. Clause 8.11 provides details on EEC authentication and authorization.

4.8 Dynamic EAS instantiation triggering

The Edge Enabler Layer can interact with the EAS management system to trigger instantiation of a suitable EAS as per application needs. Details of the EAS instantiation triggering are specified in clause 8.12.

4.9 Charging

The general architecture and principles applicable for charging of Edge enabling services provided by an ECSP to an ASP, is specified in 3GPP TS 32.240 [24].

5 Architectural requirements

5.1 General

This clause specifies architectural requirements for enabling edge applications in different functional aspects.

5.2 Architectural requirements

5.2.1 General requirements

5.2.1.1 General

This clause specifies general requirements for the architecture.

5.2.1.2 Requirements

[AR-5.2.1.2-a] The application layer architecture shall support deployment of EAS(s) and AC(s) with or without modifications compared to their existing deployments.

[AR-5.2.1.2-b] The application layer architecture shall support different deployment models in conjunction with an operator's 3GPP network.

[AR-5.2.1.2-c] The application layer architecture shall be compatible with the 3GPP network system.

5.2.2 Edge configuration data

5.2.2.1 General

This clause specifies the requirements for edge configuration data.

5.2.2.2 Requirements

[AR-5.2.2.2-a] The application layer architecture shall provide mechanisms to provide configuration parameters to an authorized EEC to access the EES(s).

5.2.3 Registration

5.2.3.1 General

This clause specifies the requirements for EEC, EAS and EES registration.

5.2.3.2 EEC registration

[AR-5.2.3.2-a] The application layer architecture shall provide mechanisms for an EEC to register onto the EES.

[AR-5.2.3.2-b] The application layer architecture shall provide mechanisms for an EEC to de-register from the EES.

[AR-5.2.3.2-c] The application layer architecture shall provide mechanisms for the EES to detect an abnormal termination of an EEC registration.

5.2.3.3 EAS registration

[AR-5.2.3.3-a] The application layer architecture shall provide mechanisms for an EAS to register to the EES.

[AR-5.2.3.3-b] The application layer architecture shall support EAS exposing its availability, which varies with time, location, etc.

[AR-5.2.3.3-c] The application layer architecture shall provide mechanisms so that the EASs are uniquely identifiable.

[AR-5.2.3.3-d] The application layer architecture shall provide mechanisms for an EAS to de-register from the EES.

[AR-5.2.3.3-e] The application layer architecture shall provide mechanisms for the EES to detect an abnormal termination of an EAS registration.

5.2.3.4 EES registration

[AR-5.2.3.4-a] The application layer architecture shall provide mechanisms for an EES to register onto the ECS.

[AR-5.2.3.4-b] The application layer architecture shall support EES to publish EAS information on the ECS.

[AR-5.2.3.4-c] The application layer architecture shall support EES to update the published EAS information on the ECS.

[AR-5.2.3.4-d] The application layer architecture shall provide mechanisms for an EES to de-register from the ECS.

[AR-5.2.3.4-e] The application layer architecture shall provide mechanisms for the ECS to detect an abnormal termination of an EES registration.

5.2.4 EAS discovery

5.2.4.1 General

This clause specifies the requirements for EAS discovery.

5.2.4.2 Requirements

[AR-5.2.4.2-a] The application layer architecture shall provide mechanisms for an EEC to discover available EASs.

[AR-5.2.4.2-b] The application layer architecture shall provide relevant configuration information of the EASs to the EEC, in order to enable communication between ACs and the EASs.

5.2.5 Capability exposure to EASs

5.2.5.1 General

This clause specifies the requirements for capability exposure to EAS.

5.2.5.2 Requirements

[AR-5.2.5.2-a] The application layer architecture shall support exposure of 3GPP network's capabilities to the EASs.

[AR-5.2.5.2-b] The application layer architecture shall support exposure of EES's capabilities to the EASs.

5.2.6 Security

5.2.6.1 General

This clause specifies the security requirements.

5.2.6.2 Requirements

[AR-5.2.6.2-a] The application layer architecture shall provide mechanisms for the Edge Computing Service Provider to authorize the usage of Edge Computing services by the EEC.

[AR-5.2.6.2-b] The application layer architecture shall provide mechanisms for the Edge Computing Service Provider to authorize the usage of Edge Computing services by the EASs.

[AR-5.2.6.2-c] Communication between the functional entities of the application layer architecture shall be protected.

[AR-5.2.6.2-d] The authentication and authorization for the use of Edge Computing services shall support the deployment where the functional entities providing the Edge Computing services are in the same trust domain as the 3GPP system, different trust domains or both.

[AR-5.2.6.2-e] The application layer architecture shall support the use of either 3GPP credentials or application specific credentials or both for different deployment needs, for the communication between the UE and the functional entities providing the Edge Computing service.

[AR-5.2.6.2-f] The application layer architecture shall support mutual authentication and authorization check between clients and servers or servers and servers that interact.

[AR-5.2.6.2-g] The application layer architecture shall support EASs to obtain user's authorization in order to access to user's sensitive information (e.g. user's location).

[AR-5.2.6.2-h] The application layer architecture shall provide mechanisms to support privacy protection of the user.

NOTE 1: Security and privacy related procedures are specified in 3GPP TS 33.558 [23].

NOTE 2: EAS obtained user consent requirement in [AR-5.2.6.2-g] is not supported in the current release.

5.2.7 Subscription service

5.2.7.1 General

This clause specifies the requirements for a subscription service.

5.2.7.2 Requirements

[AR-5.2.7.2-a] The application layer architecture shall provide subscription and notification mechanisms enabling an EEC to receive changes in dynamic information of EASs from an EES.

[AR-5.2.7.2-b] The application layer architecture shall provide subscription and notification mechanisms enabling an EEC to receive changes in availability of EASs from an EES.

[AR-5.2.7.2-c] The application layer architecture shall provide subscription and notification mechanisms enabling an EEC to receive changes in EES's information and availability status (e.g. EES endpoint change or EES is about to become unavailable due to overload, maintenance window, etc.) from an ECS.

[AR-5.2.7.2-d] The application architecture shall provide subscription and notification mechanisms enabling an EAS to receive information about relevant changes in AC(s) information of a UE.

[AR-5.2.7.2-e] The application architecture shall provide subscription and notification mechanisms enabling an EAS to receive information about relevant reports in UE location.

[AR-5.2.7.2-f] The application architecture shall provide subscription and notification mechanisms enabling to receive changes in service continuity.

5.2.8 Traffic management

5.2.8.1 General

This clause specifies the requirements for traffic management.

5.2.8.2 Requirements

[AR-5.2.8.2-a] The application layer architecture shall support AF influence on traffic routing over N6 interface.

[AR-5.2.8.2-b] The application layer architecture should be able to monitor the network status (e.g. traffic volume, throughput, network load, etc.) that may impact the application KPIs.

5.2.9 Lifecycle management

5.2.9.1 General

This clause specifies the requirements for lifecycle management.

5.2.9.2 Requirements

[A.5.2.9.2-a] The application layer architecture shall support interactions with a lifecycle management system.

5.2.10 Edge application KPIs

5.2.10.1 General

This clause specifies the requirements for edge application KPIs.

5.2.10.2 Requirements

[AR-5.2.10.2-a] The application layer architecture shall provide mechanisms for the EAS to publish its KPIs or application level requirements when available (e.g. upon new application on-boarding).

[AR-5.2.10.2-b] The application layer architecture shall provide mechanisms for the EAS to update its KPIs or application level requirements.

5.2.11 Service continuity

5.2.11.1 General

This clause specifies the requirements for service continuity.

5.2.11.2 Requirements

[AR-5.2.11.2-a] The application layer architecture shall provide mechanisms to support service continuity such that the Application Context with a S-EAS is transferred to a T-EAS.

6 Application layer architecture

6.1 General

This clause provides the overall architecture description:

- Clause 6.2 describes the functional architecture and corresponding to the functional architecture;
- Clause 6.3 describes the functional entities;
- Clause 6.4 describes the service-based interfaces;
- Clause 6.5 describes the reference points;
- Clause 6.6 describes the cardinality of functional entities and reference points; and
- Clause 6.7 describes the capabilities exposed for enabling edge applications.

6.2 Architecture

This clause describes the architecture for enabling edge applications in the following representations:

- A service-based representation, where the Edge Enabler Layer functions (e.g. ECS) enable other authorized Edge Enabler Layer functions (e.g. EES) to access their services. This representation also includes point-to-point reference points where necessary;
- A service-based representation as specified in 3GPP TS 23.501 [2], where the Network Functions (e.g. NEF) enable authorized Edge Enabler Layer functions (e.g. ECS) i.e. Application Functions, to access their services;
- A service-based representation, where the Core Network Northbound APIs as specified in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3], are utilized by authorized Edge Enabler Layer functions via CAPIF core function specified in 3GPP TS 23.222 [6]; and
- A reference point representation, where existing interactions between any two functions (e.g. EES, ECS) is shown by an appropriate point-to-point reference point (e.g. EDGE-6, EDGE-7).

Edge Enabler Layer functions shown in the service-based representation of the edge architecture shall only use service-based interfaces for their interactions.

Figure 6.2-1 illustrates the service based representation of architecture for enabling edge applications.

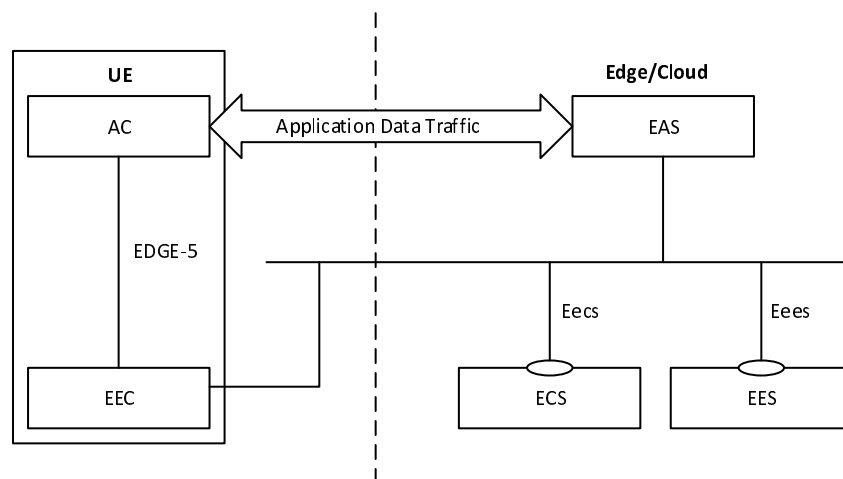


Figure 6.2-1: Architecture for enabling edge applications - service-based representation

NOTE: The EEC function and EAS function in figure 6.2-1 do not expose any service to the other functions.

Editor's note: How the possible deployment models of the ECS affect the above representation is FFS.

The mechanisms for service discovery in the service-based representation depicted in figure 6.2-1 are as follows:

- The EES discovers the ECS via pre-configuration or by using CAPIF as specified in 3GPP TS 23.222 [6];
- The EAS discovers the EES via pre-configuration or by using CAPIF as specified in 3GPP TS 23.222 [6];
- The EAS discovers the other EAS(s) as specified in clause 8.8.3.2;
- The EEC discovers the ECS as specified in clause 8.3.2; and
- The EEC discovers the EES via service provisioning as specified in clause 8.3.3.

Figure 6.2-2 illustrates the service-based representation for utilization of the 5GS network services based on the 5GS SBA specified in 3GPP TS 23.501 [2].

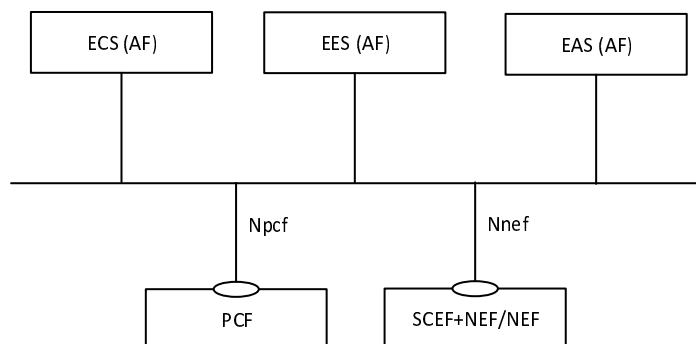


Figure 6.2-2: Utilization of 5GS network services based on the 5GS SBA – service based representation

The ECS, EES and EAS acts as AFs for consuming network services from the 3GPP 5G Core Network entities over the Service Based Architecture specified in 3GPP TS 23.501 [7].

Figure 6.2-3 illustrates the service-based representation for utilization of the Core Network (5GC, EPC) northbound APIs via CAPIF.

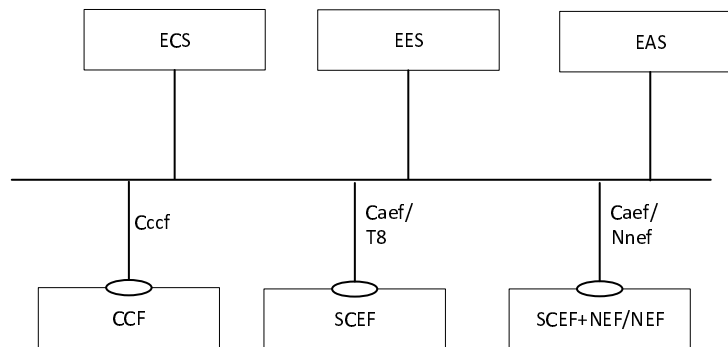


Figure 6.2-3: Utilization of Core Network Northbound APIs via CAPIF – service based representation

The ECS, EES and EAS act as authorized API invoker to consume services from the Core Network (5GC, EPC) northbound API entities like SCEF, NEF, SCEF+NEF which act as API Exposing Function as specified in 3GPP TS 23.222 [6].

The mechanism for northbound APIs discovery using the service-based interfaces depicted in figure 6.2-3 is as specified in 3GPP TS 23.222 [6].

Figure 6.2-4 illustrates the reference point representation of the architecture for edge enabling applications.

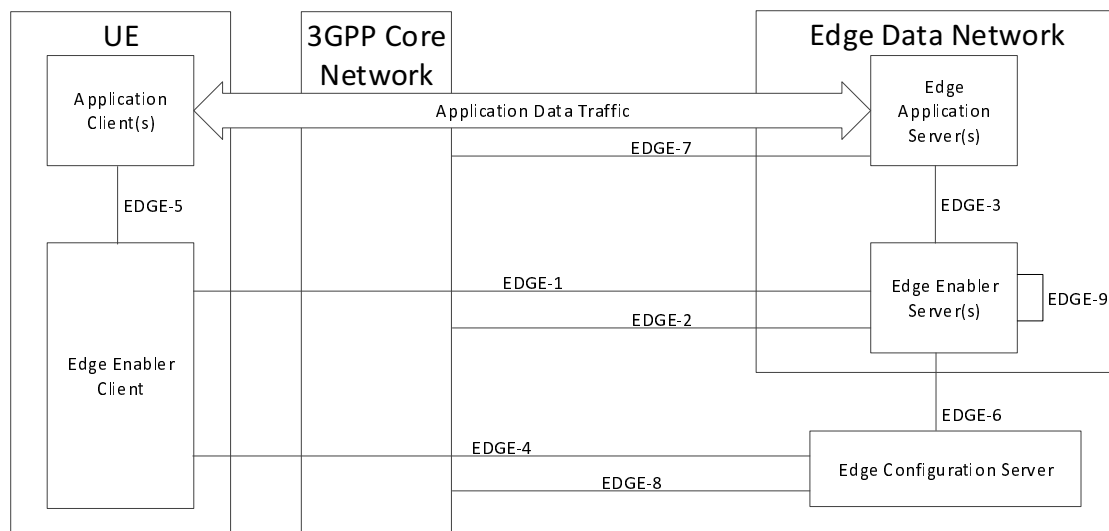


Figure 6.2-4: Architecture for enabling edge applications - reference points representation

The EDN is a local Data Network. EAS(s) and the EES are contained within the EDN. The ECS provides configurations related to the EES, including details of the EDN hosting the EES. The UE contains AC(s) and the EEC. The EAS(s), the EES and the ECS can interact with the 3GPP Core Network.

6.3 Functional entities

6.3.1 General

This clause describes the functional entities of the architecture for enabling edge applications.

6.3.2 Edge Enabler Server (EES)

EES provides supporting functions needed for EASs and EEC.

Functionalities of EES are:

- a) provisioning of configuration information to EEC, enabling exchange of application data traffic with the EAS;

- b) providing API invoker and API exposing functions as specified in 3GPP TS 23.222 [6];
- c) interacting with 3GPP Core Network for accessing the capabilities of network functions either directly (e.g. via PCF) or indirectly (i.e. SCEF/NEF/SCEF+NEF);
- d) exposing events related to ACT;
- e) EEC context transfer between EESs;
- f) supporting external exposure of 3GPP network and service capabilities to the EAS(s) over EDGE-3;
- g) registration functions (i.e., registration, update, and de-registration) for the EEC(s) and the EAS(s);
- h) triggering the EAS instantiation on demand; and
- i) supporting ACR related operations (e.g. ACR launching, ACR information notification, EELManagedACR).

6.3.3 Edge Enabler Client (EEC)

EEC provides supporting functions needed for AC(s).

Functionalities of EEC are:

- a) retrieval of configuration information to enable the exchange of Application Data Traffic with the EAS;
- b) discovery of EASs available in the EDN; and
- c) detecting UE mobility events.

6.3.4 Edge Configuration Server (ECS)

ECS provides supporting functions needed for the EEC to connect with an EES.

Functionalities of ECS are:

- a) provisioning of Edge configuration information to the EEC. The Edge configuration information includes the following:
 - 1) the information for the EEC to distinguish amongst the EESs (e.g. EDN service area); and
 - 2) the information for establishing a connection with EESs (such as URI);
- b) providing the T-EES information to the S-EES;

NOTE: The ECS can be deployed in the MNO domain or can be deployed in 3rd party domain by service provider.

- c) supporting the functionalities of registration (i.e., registration, update, and de-registration) for the EES(s);
- d) supporting the functionalities of API invoker and API exposing function as specified in 3GPP TS 23.222 [6]; and
- e) interacting with 3GPP Core Network for accessing the capabilities of network functions either directly (e.g. via PCF) or indirectly (i.e. SCEF/NEF/SCEF+NEF).

6.3.5 Application Client (AC)

AC is the application resident in the UE performing the client function. Depending on how ACR is implemented, the AC might be required to decide whether to initiate ACR. Other details of the AC are out of scope of this specification.

6.3.6 Edge Application Server (EAS)

EAS is the application server resident in the EDN, performing the server functions. The AC connects to the EAS in order to avail the services of the application with the benefits of Edge Computing.

It is possible that the server functions of an application are available only as an EAS.

However, it is also possible that certain server functions are available both at the edge and in the cloud, as an EAS and an Application Server resident in the cloud respectively. The server functions offered by an EAS and its cloud Application Server counterpart may be the same or may differ; if they differ, the Application Data Traffic exchanged with the AC may also be different.

The EAS can consume the 3GPP Core Network capabilities in the following ways, all of which are optional to support:

- a) invoking 3GPP Core Network capabilities via the edge enabler layer through the EES
- b) invoking 3GPP Core Network function (e.g. PCF) APIs directly, if it is an entity trusted by the 3GPP Core Network; and
- c) invoking the 3GPP Core Network capabilities through the capability exposure functions i.e. SCEF/NEF/SCEF+NEF.

The EAS can support processing ACR related operations (e.g. ACR status update, selected target EAS declaration).

6.4 Service-based interfaces

The architecture for enabling edge applications contains the following service-based interfaces:

Eecs: Service-based interface exhibited by ECS.

Eees: Service-based interface exhibited by EES.

6.5 Reference Points

6.5.1 General

This clause describes the reference points of the architecture for enabling edge applications.

6.5.2 EDGE-1

EDGE-1 reference point enables interactions between the EES and the EEC. It supports:

- a) registration and de-registration of the EEC to the EES;
- b) retrieval and provisioning of EAS configuration information;
- c) discovery of EASs available in the EDN; and
- d) service continuity procedures (e.g. ACR initiation).

6.5.3 EDGE-2

EDGE-2 reference point enables interactions between the EES and the 3GPP Core Network functions and APIs for retrieval of network capability information. It supports:

- access via SCEF and NEF APIs as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3], 3GPP TS 29.522 [4], 3GPP TS 23.682 [17], 3GPP TS 29.122 [5]; or
- direct access to core network functions with the EES deployed within the MNO trust domain (see 3GPP TS 23.501 [2] clause 5.13, 3GPP TS 23.503 [12], 3GPP TS 23.682 [17]).

NOTE: EDGE-2 reference point reuses 3GPP reference points or interfaces of EPS or 5GS considering different deployment models.

6.5.4 EDGE-3

EDGE-3 reference point enables interactions between the EES and the EASs. It supports:

- a) registration of EASs with availability information (e.g. time constraints, location constraints);
- b) de-registration of EASs from the EES;
- c) discovery of T-EAS information to support ACT;
- d) providing access to network capability information (e.g. location information);
- e) requesting the setup of a data session between AC and EAS with a specific QoS and receiving QoS related information; and
- f) service continuity procedures (e.g. ACR status).

NOTE: Optimized distribution of events across the EDGE-3 interface is out of scope of this specification.

6.5.5 EDGE-4

EDGE-4 reference point enables interactions between the ECS and the EEC. It supports:

- a) provisioning of Edge configuration information to the EEC.

6.5.6 EDGE-5

EDGE-5 reference point enables interactions between AC(s) and the EEC.

NOTE: Detailed specification of this reference point is out of scope of this release of this specification.

6.5.7 EDGE-6

EDGE-6 reference point enables interactions between the ECS and the EES. It supports:

- a) registration of EES information to the ECS;
- b) de-registration of EES information from the ECS; and
- c) retrieval of the T-EES information from the ECS.

6.5.8 EDGE-7

EDGE-7 reference point enables interactions between the EAS and the 3GPP Core Network functions and APIs for retrieval of network capability information. It supports:

- access via SCEF and NEF APIs as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3], 3GPP TS 29.522 [4], 3GPP TS 23.682 [17], 3GPP TS 29.122 [5]; or
- direct access to core network functions with the EAS deployed within the MNO trust domain (see 3GPP TS 23.501 [2] clause 5.13, 3GPP TS 23.682 [17]).

NOTE: EDGE-7 reference point reuses 3GPP reference points or interfaces of EPS or 5GS considering different deployment models.

6.5.9 EDGE-8

EDGE-8 reference point enables interactions between the ECS and the 3GPP Core Network functions and APIs for retrieval of network capability information. It supports:

- access via SCEF and NEF APIs as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3], 3GPP TS 29.522 [4], 3GPP TS 23.682 [17], 3GPP TS 29.122 [5]; or

- direct access to core network functions with the ECS deployed within the MNO trust domain (see 3GPP TS 23.501 [2] clause 5.13, 3GPP TS 23.682 [17]).

NOTE: EDGE-8 reference point reuses 3GPP reference points or interfaces of EPS or 5GS considering different deployment models.

6.5.10 EDGE-9

EDGE-9 reference point enables interactions between two EESs. EDGE-9 reference point may be provided between EES within different EDN (Figure 6.5.10-1) and within the same EDN (Figure 6.5.10-2).

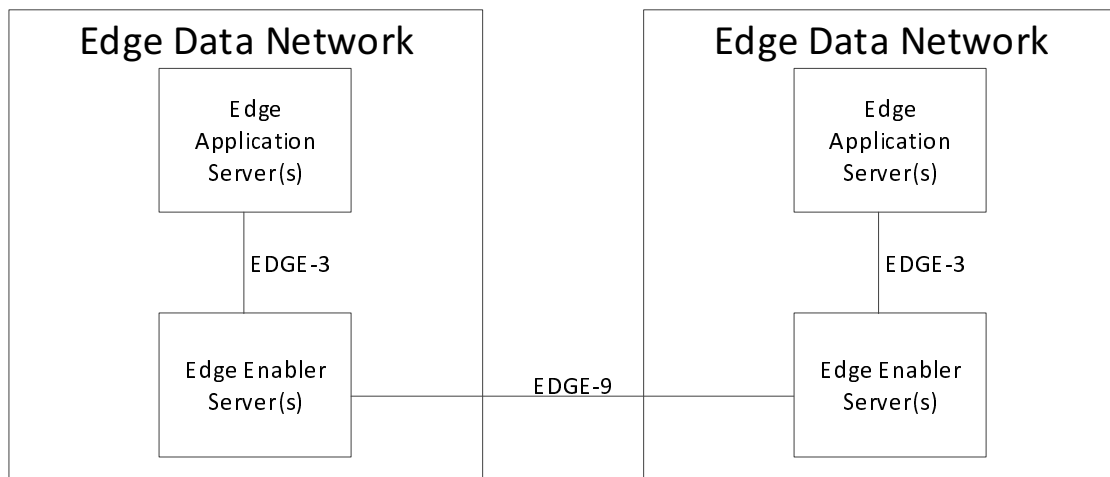


Figure 6.5.10-1: Inter-EDN EDGE-9

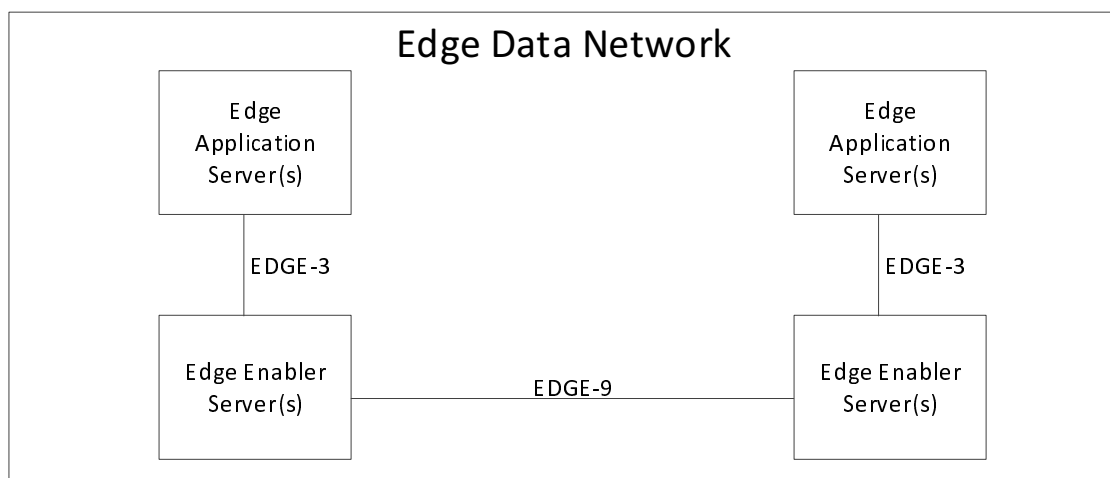


Figure 6.5.10-2: Intra-EDN EDGE-9

EDGE-9 supports:

- discovery of T-EAS information to support ACR;
- EEC context relocation procedures; and
- transparent transfer of the application context during EELManagedACR.

6.6 Cardinality rules

6.6.1 General

The cardinality rules are applied to the architecture specified in clause 6.2. The cardinality rules are classified as functional entity cardinality and reference point cardinality. The functional entity cardinality specifies the multiplicity of the functional entity that can exist as per the architecture. The reference point cardinality specifies the multiplicity of source and target functional entities that can exist in a relationship defined by the reference point in the architecture.

NOTE: The cardinality rules for the functional entities involved in EDGE-2, EDGE-7 and EDGE-8 interactions with 3GPP core network is based on the interactions between the AF and 3GPP Core Network entities as specified in 3GPP TS 23.501 [2] and 3GPP TS 23.682 [17].

6.6.2 Functional Entity Cardinality

6.6.2.1 General

6.6.2.2 AC

The following cardinality rules apply for ACs:

- a) one or more ACs may be located in a UE.

6.6.2.3 EEC

The following cardinality rules apply for EECs:

- a) One or more EEC(s) may be located in a UE.

6.6.2.4 ECS

The following cardinality rules apply for ECSs:

- a) One or more ECS(s) may be deployed to support one EDN;
- b) One ECS may be deployed to support one or more EDN(s);
- c) One or more ECS(s) may be deployed by a PLMN operator; and
- d) One or more ECS(s) may be deployed by an ECSP.

6.6.2.5 EES

The following cardinality rules apply for EES:

- a) One or more EES(s) may be located in an EDN; and
- b) One or more EES(s) may be located in an EDN per ECSP.

6.6.2.6 EAS

The following cardinality rules apply for EASs:

- a) One or more EAS(s) may be located in an EDN.

NOTE: EAS(s) belonging to the same EASID can be deployed with EES(s) of multiple ECSP(s) in an EDN.

6.6.3 Reference Point Cardinality

6.6.3.1 General

6.6.3.2 EDGE-1 (Between EEC and EES)

The following cardinality rules apply for EDGE-1:

- a) One EEC may communicate with one or more EES(s) for one or more AC concurrently; and
- b) One EES may communicate with one or more EEC(s) concurrently.

6.6.3.3 EDGE-3 (Between EAS and EES)

The following cardinality rules apply for EDGE-3:

- a) One EAS may communicate with only one EES within the same EDN; and
- b) One EES may communicate with one or more EAS(s) concurrently.

6.6.3.4 EDGE-4 (Between EEC and ECS)

The following cardinality rules apply for EDGE-4:

- a) One EEC may communicate with one or more ECS(s) concurrently; and
- b) One ECS may communicate with one or more EEC(s) concurrently.

6.6.3.5 EDGE-5 (Between AC and EEC)

The following cardinality rules apply for EDGE-5:

- a) One AC may communicate with only one EEC; and
- b) One EEC may communicate with one or more AC(s) concurrently.

6.6.3.6 EDGE-6 (Between EES and ECS)

The following cardinality rules apply for EDGE-6:

- a) One EES may communicate with one or more ECS(s) concurrently; and
- b) One ECS may communicate with one or more EES(s) concurrently.

6.6.3.7 EDGE-9 (Between EES and EES)

The following cardinality rules apply for EDGE-9:

- a) One EES may communicate with one or more EES(s) concurrently.

6.7 Capability exposure for enabling edge applications

6.7.1 General

The Figure 6.7.1-1 shows the capability exposure for enabling edge applications.

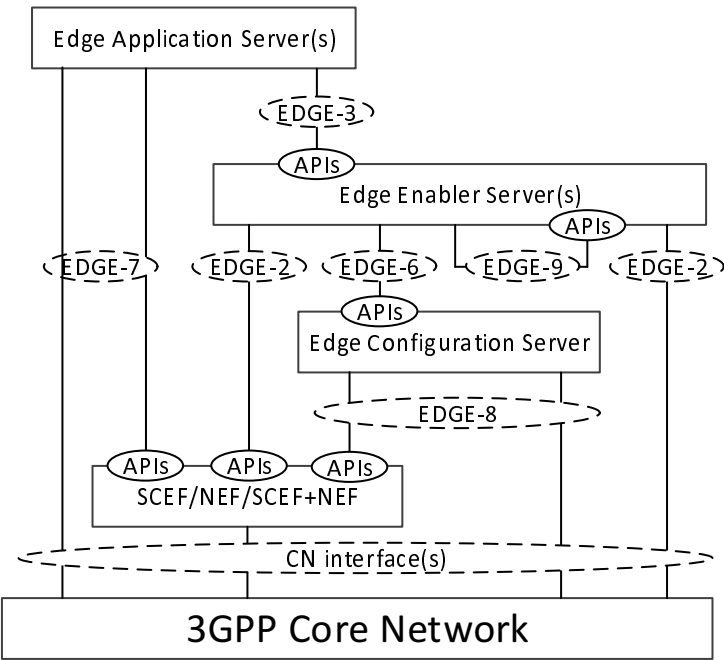


Figure 6.7.1-1: Capability exposure for enabling edge applications

Capability exposure includes the 3GPP core network (i.e. 5GC, EPC), ECS and the EES capability exposure, to fulfil the needs of the edge service operations. The capability exposure functionality is utilized by the functional entities (i.e. EES, EAS and ECS) depicted in the architecture for enabling the edge applications.

6.7.2 APIs provided by the Edge Enabler Layer

Table 6.7.2-1 summarizes the APIs exposed by the ECS.

Table 6.7.2-1: APIs provided by the ECS

API Name	Known Consumers	References
Eecs_ServiceProvisioning	EEC	8.3
Eecs_EESRegistration	EES	8.4.4
Eecs_TargetEESDiscovery	EES	8.8.3.3

Table 6.7.2-2 summarizes the APIs exposed the EES.

Table 6.7.2-2: APIs provided by the EES

API Name	Known Consumers	References
Eees_EECRegistration	EEC	8.4.2
Eees_EASRegistration	EAS	8.4.3
Eees_EASDiscovery	EEC	8.5
Eees_UELocation	EAS	8.6.2
Eees_ACRManagementEvent	EAS	8.6.3
Eees_AppClientInformation	EAS	8.6.4
Eees_UIIdentifier	EAS	8.6.5
Eees_SessionWithQoS	EAS	8.6.6
Eees_TargetEASDiscovery	EAS, EES	8.8.3.2
Eees_AppContextRelocation	EEC, EAS	8.8.3.4
Eees_ACREvents	EEC	8.8.3.5
Eees_EELManagedACR	EAS	8.8.3.6
Eees_EECContextPull	EES	8.9.4.2
Eees_EECContextPush	EES	8.9.4.3
Eees_SelectedTargetEAS	EAS	8.8.3.7
Eees_ACRStatusUpdate	EAS	8.8.3.8

NOTE: The event exposure related APIs (e.g. Eees_EASDiscovery and Eees_ACREvents) can be realized as single event subscription API.

7 Identities and commonly used values

7.1 General

The following clauses list identities and commonly used values that are used in this technical specification.

7.2 Identities

7.2.1 General

The following clauses specify a collection of identities that are associated with entities defined and being used in this specification.

7.2.2 Edge Enabler Client ID (EECID)

The EECID is a globally unique value that identifies an EEC.

NOTE: Security and privacy aspects related to EECID are specified in 3GPP TS 33.558 [23].

7.2.3 Edge Enabler Server ID (EESID)

The EESID identifies an EES and each EESID is unique within PLMN domain.

7.2.4 Edge Application Server ID (EASID)

The EASID identifies a particular application for e.g. SA6Video, SA6Game etc. For example, all Edge SA6Video Servers will share the same EASID.

NOTE: The definition of the EASID is out of scope of this specification.

7.2.5 Application Client ID (ACID)

The ACID identifies the client side of a particular application, for e.g. SA6Video viewer, SA6MsgClient etc. For example, all SA6MsgClient clients will share the same ACID.

In case that the UE is running mobile OS, the ACID is a pair of OSId and OSAppId.

7.2.6 UE ID

The UE ID uniquely identifies a particular UE within a PLMN domain. Following identities are examples that can be used:

- a) GPSI, as defined in 3GPP TS 23.501 [2].

NOTE: To protect privacy of the user, MSISDN can be used as GPSI only after obtaining user's consent.

7.2.7 UE Group ID

The UE Group ID uniquely identifies a group of UE within a PLMN domain. Following identities are examples that can be used:

- a) internal group ID, as defined in 3GPP TS 23.501 [2]; and
- b) external group ID, as defined in 3GPP TS 23.501 [2].

7.2.8 EEC Context ID

The EEC Context ID is a globally unique value which identifies a set of parameters associated with the EEC (e.g., due to registration) and maintained in the Edge Enabler Layer by EESs.

If the EEC registration request does not include a previously assigned EEC Context ID value, the receiver EES assigns a new EEC Context ID and creates an EEC Context as described in the Table 8.2.8-1.

Providing a previously assigned EEC Context ID at registration allows maintaining the EEC Context in the Edge Enabler Layer beyond the lifetime of a registration, subject to policies. If the EEC registration request does include a previously assigned EEC Context ID value, after EEC Context relocation, the receiver EES may assign a new EEC Context ID, subject to implementation and local policies.

NOTE: The EEC Context ID may be implemented as combination of other IDs (e.g., EES ID and registration ID). How the EEC Context ID is specified or assigned is out of scope of this specification.

7.3 Commonly used values

7.3.1 General

7.3.2 UE location

The UE location identifies where the UE is connected to the network or the position of the UE. It provides consistent definition of the UE's location across the UE and network entities. Following values are examples of UE locations that can be used:

- a) Cell Identity, Tracking Area Identity, GPS Coordinates or civic addresses as defined in 3GPP TS 23.502 [3] clause 4.15.3.

7.3.3 Service areas

7.3.3.1 General

ECSPs and ASPs may allow access to Edge Computing service from specific areas i.e. allowing only the UEs within that area to access functional entities resident in the EDN. This area is called service area.

Some functional elements make decisions based on the topological location of the UE, (e.g. the cell it is connected to) while others make decisions based on the UE's geographical location (e.g. its geographical coordinates).

Functional elements that are aware of both topological and geographical information can translate one value to the other.

7.3.3.2 Topological Service Area

A Topological Service Area is defined in relationship with a UE's point of connection to the network, such as: a collection of Cell IDs, Tracking Area Identities or the PLMN ID. Any UE that is attached to the Core Network from a cell whose ID is in this list, can be served by the functional entity in the EDN that is configured to serve that Topological Service Area.

NOTE: Topological Service Area information is not applicable for untrusted functional elements (EESs and/or EASs deployed outside the MNO trust domain).

7.3.3.3 Geographical Service Area

A Geographical Service Area is an area that is specified by geographical units as defined in 3GPP TS 23.032 [21], such as: Geographical coordinates, an area that is defined as a circle whose centre is denoted by geographical coordinates, an area that is defined by a polygon whose corners are denoted by geographical coordinates. A Geographical Service Area can also be expressed in other ways such as: a well-known buildings, parks, arenas, civic addresses or ZIP code etc.

Applications can be configured to serve UEs that are in a specified geographical area and deny service from UEs that are not located in that area.

NOTE: Whether and how geographical information is used by applications to provide or deny service is out of scope.

7.3.3.4 EDN service area

A service area from which the access to the EDN is allowed. ECSPs can use LADNs, as described in Annex A.2.4 of this document, to deploy EDNs with access restricted from specific areas. When an EDN is deployed using LADN, the EDN service area is same as the LADN service area and rules specified for LADN apply to the UE, as specified in 3GPP TS 23.501 [2].

In a deployment using DNs other than LADNs, the EDN service area is the whole PLMN for non-roaming scenario.

NOTE 1: The EDN service area for roaming scenario is out of scope in this release of the specification.

NOTE 2: For the purpose of restricting the access to the EES from specific areas, ECSP can use the EES service area, which is specified in clause 7.3.3.5, even if the EDN service area is the whole PLMN.

The EDN service area may be expressed as a Topological Service Area.

7.3.3.5 EES Service Area

A service area from which the access to the EES is allowed. This service area is equal to or a subset of the service area of the EDN in which the EES resides.

The EES service area may be expressed as a Topological Service Area, a Geographical Service Area or both.

7.3.3.6 EAS service area

A service area from which the access to the EAS is allowed. This service area is equal to or a subset of the service area of the EES which serves the EAS.

The EAS service area may be expressed as a Topological Service Area, a Geographical Service Area or both.

8 Procedures and information flows

8.1 General

This clause provides procedures and information flows necessary for enabling edge application including information elements used in the procedures.

8.2 Common Information Elements

8.2.1 General

This clause provides descriptions for Information Elements which are commonly used in several procedures.

8.2.2 AC Profile

An AC Profile includes information about AC used to determine services and service characteristics required.

Table 8.2.2-1: AC Profile

Information element	Status	Description
ACID	M	Identity of the AC.
AC Type	O	The category or type of AC (e.g. V2X). This is an implementation specific value.
Preferred ECSP list	O	When used in a service provisioning request, this IE indicates to the ECS which ECSPs are preferred for the AC. The ECS may use this information in the selection of EESs.
AC Schedule	O	The expected operation schedule of the AC (e.g. time windows)
Expected AC Geographical Service Area	O	The expected location(s) (e.g. route) of the hosting UE during the AC's operation schedule. This geographic information can express a geographic point, polygon, route, signalling map, or waypoint set.
AC Service Continuity Support	O	Indicates if service continuity support is required or not for the application. The IE also indicates which ACR scenarios are supported by the AC and which of these are preferred by the AC.
List of EASs	O	List of EAS that serve the AC along with the service KPIs required by the AC
> EASID	M	Identifier of the EAS
> Expected AC Service KPIs	O	KPIs expected in order for ACs to receive currently required services from the EAS, as described in Table 8.2.3-1
> Minimum required AC Service KPIs	O	Minimum KPIs required in order for ACs to receive meaningful services from the EAS, as described in Table 8.2.3-1

8.2.3 AC Service KPIs

AC Service KPIs provide information about service characteristics required by the ACs.

Table 8.2.3-1: AC Service KPI

Information element	Status	Description
Connection bandwidth	O	The required connection bandwidth in Kbit/s for the application.
Request rate	O	The request rate to be generated by the AC.
Response time	O	Response time (NOTE) required for the server servicing the requests.
Availability	O	Percentage of time the server is required to be available for the AC's use.
Compute	O	The compute resources required by the AC.
Graphical Compute	O	The graphical compute resources required by the AC.
Memory	O	The memory resources required by the AC.
Storage	O	The storage resources required by the AC.
NOTE: The response time includes the round-trip time of the request and response packet, the processing time at the server and the time required by the server to consume 3GPP Core Network capabilities, if any.		

8.2.4 EAS Profile

Table 8.2.4-1: EAS Profile

Information element	Status	Description
EASID	M	The identifier of the EAS
EAS Endpoint	M	Endpoint information (e.g. URI, FQDN, IP address) used to communicate with the EAS. This information may be discovered by EEC and exposed to ACs so that ACs can establish contact with the EAS.
ACID(s)	O	Identifies the AC(s) that can be served by the EAS
EAS Provider Identifier	O	The identifier of the ASP that provides the EAS.
EAS Type	O	The category or type of EAS (e.g. V2X)
EAS description	O	Human-readable description of the EAS
EAS Schedule	O	The availability schedule of the EAS (e.g. time windows)
EAS Geographical Service Area	O	The geographical service area that the EAS serves. ACs in UEs that are located outside that area shall not be served.
EAS Topological Service Area	O	The EAS serves UEs that are connected to the Core Network from one of the cells included in this service area. ACs in UEs that are located outside this area shall not be served. See possible formats in Table 8.2.7-1.
EAS Service KPIs	O	Service characteristics provided by EAS, detailed in Table 8.2.5-1
EAS service permission level	O	Level of service permissions e.g. trial, gold-class supported by the EAS
EAS Feature(s)	O	Service features e.g. single vs. multi-player gaming service supported by the EAS
EAS Service continuity support	O	Indicates if the EAS supports service continuity or not. This IE also indicates which ACR scenarios are supported by the EAS.
List of EAS DNAI(s)	O	DNAI(s) associated with the EAS. This IE is used as Potential Locations of Applications in clause 5.6.7 of 3GPP TS 23.501 [2]. It is a subset of the DNAI(s) associated with the EDN where the EAS resides.
List of N6 Traffic Routing requirements	O	The N6 traffic routing information and/or routing profile ID corresponding to each EAS DNAI.
EAS Availability Reporting Period	O	The availability reporting period (i.e. heartbeat period) that indicates to the EES how often it needs to check the EAS's availability after a successful registration.
EAS Status	O	The status of the EAS (e.g. enabled, disabled, etc.)

8.2.5 EAS Service KPIs

EAS Service KPIs provide information about service characteristics provided by the EAS

Table 8.2.5-1: EAS Service KPIs

Information element	Status	Description
Maximum Request rate	O	Maximum request rate from the AC supported by the server.
Maximum Response time	O	The maximum response time advertised for the AC's service requests.
Availability	O	Advertised percentage of time the server is available for the AC's use.
Available Compute	O	The maximum compute resource available for the AC.
Available Graphical Compute	O	The maximum graphical compute resource available for the AC.
Available Memory	O	The maximum memory resource available for the AC.
Available Storage	O	The maximum storage resource available for the AC.
Connection Bandwidth	O	The connection bandwidth in Kbit/s advertised for the AC's use.
NOTE: The maximum response time includes the round-trip time of the request and response packet, the processing time at the server and the time required by the server to consume 3GPP Core Network capabilities, if any.		

8.2.6 EES Profile

The EES profile includes information about the EES and the services it provides.

Table 8.2.6-1: EES Profile

Information element	Status	Description
EESID	M	The identifier of the EES
EES Endpoint	M	Endpoint information (e.g. URI, FQDN, IP address) used to communicate with the EES. This information is provided to the EEC to connect to the EES.
EASIDs	M	List of EASIDs registered with the EES.
EEC registration configuration	M	Indicates whether the EEC is required to register on the EES to use edge services or not.
EES Provider Identifier	O	The identifier of the ECSP that provides the EES Provider.
EES Topological Service Area	O	The EES serves UEs that are connected to the Core Network from one of the cells included in this service area. EECs in UEs that are located outside this area shall not be served. See possible formats in Table 8.2.7-1.
EES Geographical Service Area	O	The area being served by the EES in Geographical values (as specified in clause 7.3.3.3)
List of EES DNAI(s)	O	DNAI(s) associated with the EES. This IE is used as Potential Locations of Applications in clause 5.6.7 of 3GPP TS 23.501 [2]. It is a subset of the DNAI(s) associated with the EDN, where the EES resides.
EES Service continuity support	O	Indicates if the EES supports service continuity or not. This IE also indicates which ACR scenarios are supported by the EES.

NOTE: The list of EES DNAI(s) can include the DNAI(s) of the EAS(s) registered with the EES.

8.2.7 Topological Service Area

The following formats may be used for expressing a Topological Service Area:

Table 8.2.7-1: Topological Service Area

Information element	Status	Description
Cell IDs (NOTE)	O	The list of cell IDs defining the Topological Service Area
TAIs (NOTE)	O	The list of Tracking Area IDs defining the Topological Service Area
PLMN IDs (NOTE)	O	The list of PLMN IDs defining the Topological Service Area
NOTE: A combination of these information elements can be used to define the Topological Service Area. Combinations should not have duplicate or overlapping information for the same Topological Service Area.		

8.2.8 EEC Context

The EEC Context includes information about an EEC for receiving edge enabler services.

Table 8.2.8-1: EEC Context

Information element	Status	Description
EEC ID	M	Unique identifier of the EEC.
EEC Context ID	M	Identifier assigned to the EEC Context
Source EES Endpoint	M	The endpoint address (e.g., URI, IP address) of the EES that provided EEC context ID.
UE Identifier	O	The identifier of the hosting UE (i.e., GPSI or identity token)
List of EDGE-1 subscriptions	O	List of subscriptions IDs for capability exposure to the EEC ID (NOTE).
UE location	O	Latest UE location of the UE hosting the EEC which was available at the EES.
List of AC Profiles	O	Information about the ACs as described in Table 8.2.2-1.
List of Service Session Contexts	O	List of associated Service Session Context IEs. Each Service Session Context includes information maintained by the EES for the services (involving UE related resources) received from an EAS registered to the EES.
> Service Session Context	M	Service Session Context is described in Table 8.2.8-2
NOTE: The corresponding EDGE-1 subscription information may include 3GPP CN subscription information such as subscription correlation ID		

Table 8.2.8-2: Service Session Context

Information element	Status	Description
EAS ID	M	Identifier of the EAS providing the application services
EAS Endpoint	M	Endpoint information of the EAS.
AC ID	O	Identifier of the AC ID for which the service session is provided, if determined.

Editor's Note: It is FFS whether the EEC Context information captured in table 8.2.8-1 requires further updates and alignment to include EDGE-3 subscription information.

8.2.9 Geographical Service Area

The following formats may be used for expressing a Geographical Service Area:

Table 8.2.9-1: Geographical Service Area

Information element	Status	Description
Geographical Area Description	O	A shape defined in 3GPP TS 23.032 [21]
Civic Location	O	An area identified by a civic location element, e.g. building, park, arena, civic address or ZIP code.

8.3 ECS Discovery and Service provisioning

8.3.1 General

Service provisioning allows configuring the EEC with information about available Edge Computing services, based on the hosting UEs location, service requirements, service preferences and connectivity. This configuration includes the necessary address information for the EEC to establish connection with the EES(s).

If the ECS deployed by MNO is contracted with one or more ECSP(s), the ECS provides EES configuration information of MNO owned and ECSP owned EESs via MNO ECS as described in clause 8.3.3.3.3.

If the ECS is deployed by a non-MNO ECSP, the ECS endpoint address may be configured with the EEC. An EEC that is aware of multiple ECSP's ECS endpoint addresses may perform the service provisioning procedure per ECS of each ECSP multiple times.

Figure 8.3.1-1 illustrates an overview of service provisioning. Service provisioning procedures support the following models:

- Request/Response model; and
- Subscribe/Notify model.

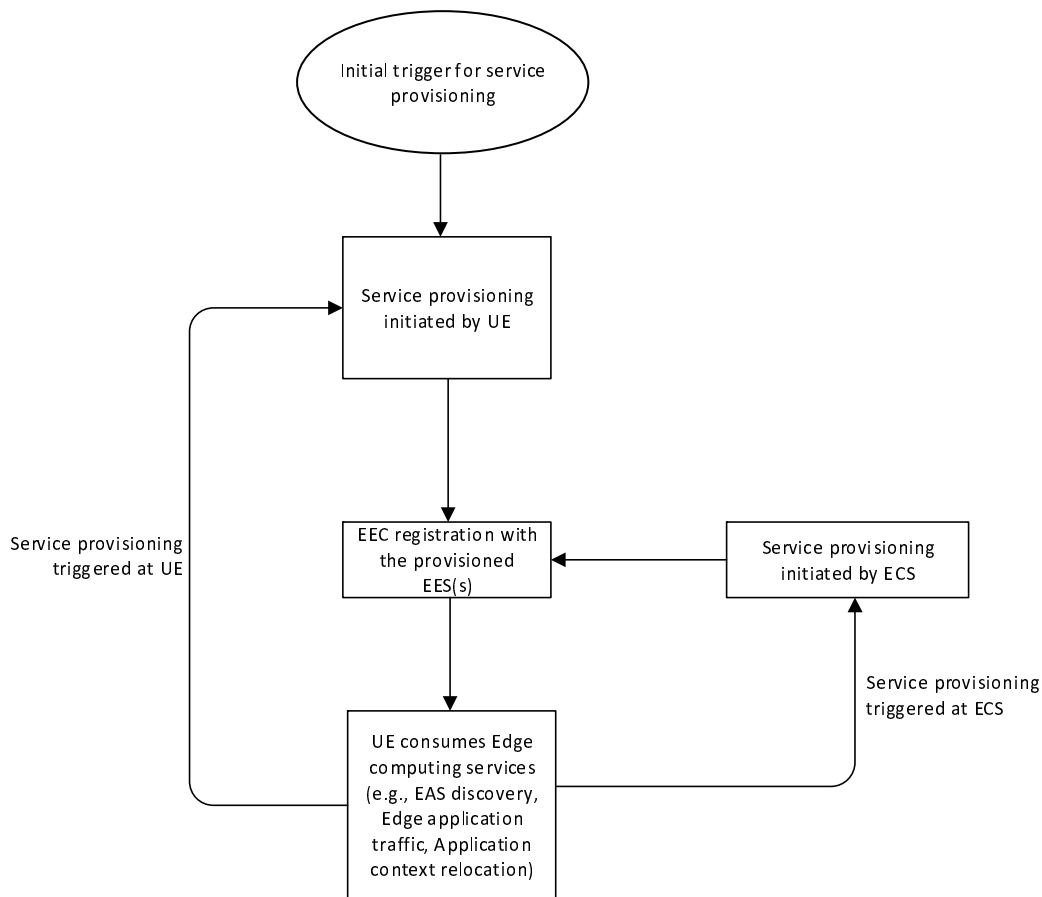


Figure 8.3.1-1: Overview of Service provisioning

The UE is initially provisioned from the ECS with the configurations required to connect to the EDN. Once provisioned, the EEC of the UE registers with the selected EES(s) from the list of provisioned EES(s) it received from the ECS(s), if the EEC registration configuration in EES profile indicates that EEC registration is required. The UE further consumes the edge computing services and performs various operations such as EAS discovery, Edge application communications, ACR, etc. While the UE is consuming the edge computing services, there may be several triggers which may cause service provisioning to be triggered by the UE or by the ECS.

The triggers for service provisioning are classified as:

a. Triggers at UE - Some examples are:

- AC related updates available at the EEC due to AC installation/re-installation, AC requesting application server access (e.g. via internet browser);
- EEC supporting one or more ACs may be updated due to EEC re-installation; and
- Lifetime of EDN Configuration Information is expired or the EEC detects that the UE moves out of EDN Service Area in the EDN Configuration Information.

b. Triggers at ECS – Some examples are:

- EES updates received due to EAS installation/re-installation/re-location; and
- ECS receives the EDN/DNAI change notification of the UE from 5GC when the ECS subscribes to the user plane path management events as specified in clause 8.10.2.

8.3.2 ECS Discovery

8.3.2.1 General

ECS configuration information consists of one or more endpoint information (e.g. URI(s), FQDN(s), IP address(es)) of ECS(s), and optionally the corresponding ECS Provider Identifier. ECS configuration information can be

- pre-configured with the EEC;
- configured by an edge-aware AC;
- configured by the user;
- provisioned by MNO through 5GC procedure if the UE has the capability to deliver the ECS configuration information to the EEC on the UE (see 3GPP TS 23.548 [20], clause 6.5.2); or
- derived from HPLMN identifier for non-roaming scenario or from VPLMN identifier for roaming scenario.

NOTE: How the ECS configuration information is configured to the EEC by the AC, user, or pre-configuration is out of scope of the present specification.

It may be possible to provide the ECS configuration information to the EEC from the 5GC if the UE has the capability to deliver the ECS configuration information to the EEC on the UE.

If the ECS configuration information is provided by 5GC and available at the EEC, the EEC shall use the information for the initial provisioning request. Otherwise, the EEC shall use pre-configured ECS address for the initial provisioning if ECS configuration information is preconfigured with the EEC.

Table 8.3.2.1-1 describes the information elements of ECS configuration information for an ECS.

Table 8.3.2.1-1: ECS configuration information per ECS

Information element	Status	Description
ECS address	M	Endpoint information of ECS (e.g. URI, FQDN, IP address)
ECSP Identifier	O	The identifier of the ECSP (e.g., the MNO or a 3rd party service provider) that provides the ECS.
Spatial Validity Conditions	O	Spatial validity condition, as described in 3GPP TS 23.548 [20]
NOTE: This IE shall be included when the ECS configuration information is provisioned by the MNO through the 5GC procedure.		

Editor's Note: Information Elements of ECS configuration information are FFS.

8.3.2.2 Procedures

8.3.2.2.1 General

There is no additional information about procedures for ECS Discovery.

8.3.2.3 Information flows

8.3.2.3.1 General

There is no additional information about information flows for ECS Discovery

8.3.2.4 APIs

8.3.2.4.1 General

There is no additional information about APIs for ECS Discovery

8.3.3 Service provisioning

8.3.3.1 General

The following clauses specify procedures, information flows and APIs for service provisioning.

8.3.3.2 Procedures

8.3.3.2.1 General

Following procedures are supported for service provisioning:

- Request-response procedure;
- Subscribe-notify procedures, including:
 - Subscription procedure;
 - Notification procedure;
 - Subscription update procedure; and
 - Unsubscribe procedure.

8.3.3.2.2 Request-response model

Figure 8.3.3.2.2-1 illustrates service provisioning procedure based on request/response model.

Pre-conditions:

1. The EEC has been pre-configured or has discovered the address (e.g. URI) of the ECS;
2. The EEC has been authorized to communicate with the ECS;
3. The UE Identifier is either preconfigured or resulted from a successful authorization; and
4. The ECS is configured with ECSP's policy for service provisioning.

NOTE 1: Details of ECSP's policy are out of scope.

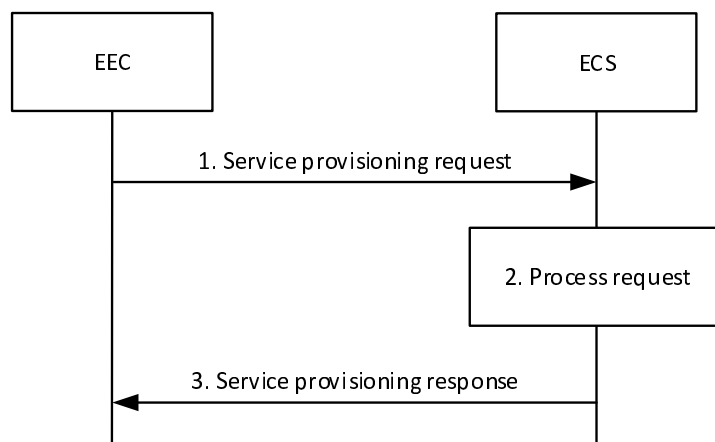


Figure 8.3.3.2.2-1: Service provisioning – Request/Response

1. The EEC sends a service provisioning request to the ECS. The service provisioning request includes the security credentials of the EEC received during EEC authorization procedure and may include the UE identifier such as GPSI, connectivity information, UE location and AC profile(s) information.
2. Upon receiving the request, the ECS performs an authorization check to verify whether the EEC has authorization to perform the operation. The ECS may utilize the capabilities (e.g. UE location) of the 3GPP core network as specified in clause 8.10.2. If AC profile(s) are provided by the EEC, the ECS identifies the EES(s) based on the provided AC profile(s) and the UE location. When AC profiles(s) are not provided, then:
 - if available, the ECS identifies the EES(s) based on the UE-specific service information at the ECS and the UE location;
 - ECS identifies the EES(s) by applying the ECSP policy (e.g. based only on the UE location);

NOTE 2: Details of the UE-specific service information and how it is available at the ECS is out of scope.

NOTE 3: Both steps are evaluated prior to sending a response.

The ECS also determines other information that needs to be provisioned, e.g. identification of the EDN, EDN service area, EES endpoints.

3. If the processing of the request was successful, the ECS responds to the EEC's request with a service provisioning response which includes a list of EDN configuration information, e.g. identification of the EDN, EDN service area, and the required information (e.g. URI, IP address) for establishing a connection to the EES.

If the ECS is not provisioned with any EDN configuration information or is unable to determine the EES information using the inputs in service provisioning request, UE-specific service information at the ECS or the ECSP's policy, the ECS shall reject the service provisioning request and respond with an appropriate failure cause.

If the EDN configuration information includes an LADN DNN as an identifier for the EDN, the EEC considers the LADN as the EDN. Therefore, the service area of EDN is the LADN Service Area which can be discovered using the UE Registration Procedure.

The EEC may cache the service provisioning information (e.g. EES endpoint) for subsequent use and avoid the need to repeat step 1. If the Lifetime IE is included in the Service provisioning response, then the EEC may cache and reuse the Service provisioning information only for the duration specified by the Lifetime IE, without the need to repeat step 1.

If the ECS provided information regarding the service continuity support of individual EESs, the EEC may take this information into account when selecting an EES for EEC registration, EAS discovery or T-EAS discovery, respectively.

NOTE 4: If the service provisioning request fails, the EEC can resend the service provisioning request again, taking into account the received failure cause.

NOTE 5: Even after the EEC establishes a connection to the EES using information received in step 3, the EES can issue AF request to influence traffic routing from EEC to EES as specified in 3GPP TS 23.501 [2] clause 5.6.7.

8.3.3.2.3 Subscribe-notify model

8.3.3.2.3.1 General

Clause 8.3.3.2.3.2 and clause 8.3.3.2.3.3 together illustrate the service provisioning procedure based on Subscribe/Notify model.

Clause 8.3.3.2.3.4 illustrates the service provisioning update procedure.

Clause 8.3.3.2.3.5 illustrates the service provisioning unsubscribe procedure.

8.3.3.2.3.2 Subscribe

Figure 8.3.3.2.3.2-1 illustrates the service provisioning subscription procedure between the EEC and the ECS.

Pre-conditions:

1. The EEC has been pre-configured or has discovered the address (e.g. URI) of the ECS;
2. The EEC has been authorized to communicate with the ECS as specified in clause 8.11;
3. The UE Identifier is either preconfigured or resulted from a successful authorization;
4. The ECS is configured with ECSP's policy for service provisioning; and
5. The EEC has optionally acquired a Notification Target Address to be used in its subscriptions to notifications.

NOTE 1: Details of ECSP's policy are out of scope.

NOTE 2: How the EEC acquires the notification target address or a notification channel URI to receive the notifications is out of scope of this release. The notification target address can terminate at the EEC (e.g. in an IoT device) if the deployment supports EEC reachability, or it can terminate at a push notification service. Details of the push notification service are out of scope of this release.

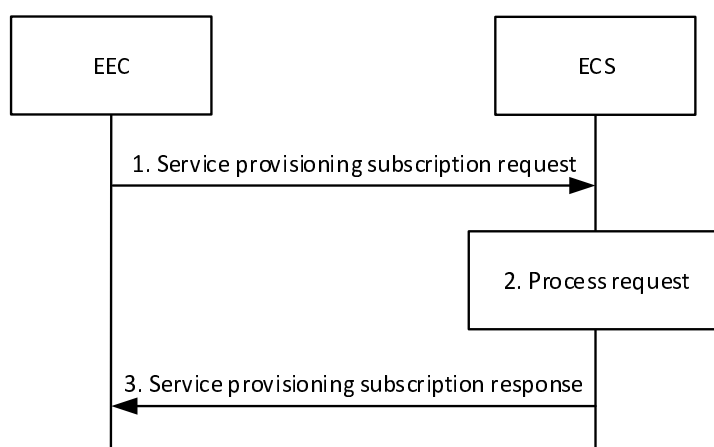


Figure 8.3.3.2.3.2-1: Service provisioning subscription

1. The EEC sends a service provisioning subscription request to the ECS. The service provisioning subscription request includes the security credentials of the EEC received during EEC authorization procedure and Notification Target Address (e.g. URL) and may include the UE identifier such as GPSI, connectivity information, proposed expiration time and AC Profile information.
2. Upon receiving the request, the ECS performs an authorization check to verify whether the EEC has authorization to perform the operation. If required, the ECS may utilize the capabilities (e.g. UE location or user plane management event notification service if available) of the 3GPP core network as specified in clause 8.10.2. If the request is authorized, the ECS creates and stores the subscription for provisioning.

NOTE 3: The ECS can monitor the user plane path change for EDGE-1 traffic toward EES(s) by utilizing the user plane management event notification service specified in 3GPP TS 23.501 [2]. Based on target DNAI reported from 5GC the ECS can notify more suitable EES(s) to the EEC.

3. If the processing of the request was successful, the ECS responds with a service provisioning subscription response, which includes the subscription identifier and may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the EEC shall send a Service provisioning subscription update request prior to the expiration time. If a Service provisioning subscription update request is not received prior to the expiration time, the ECS shall treat the EEC as implicitly unsubscribed.

If the ECS is unable to determine the EES information using the inputs in service provisioning subscription request, UE-specific service information at the ECS or the ECSP policy, the ECS shall reject the service provisioning subscription request and respond with an appropriate failure cause.

NOTE 4: If the service provisioning subscription request fails, the EEC can resend the service provisioning subscription request again, taking into account the received failure cause.

8.3.3.2.3.3 Notify

Figure 8.3.3.2.3.3-1 illustrates the service provisioning notification procedure between the EEC and the ECS.

Pre-conditions:

1. The EEC has subscribed with the ECS for the provisioning information as specified in clause 8.3.3.2.3.2.

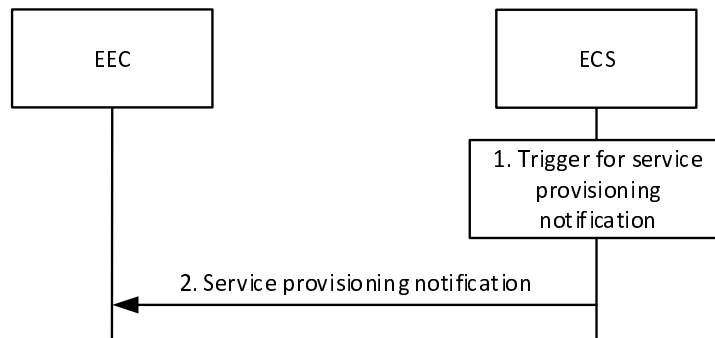


Figure 8.3.3.2.3.3-1: Service provisioning notification

1. An event occurs at the ECS that satisfies trigger conditions for updating service provisioning of a subscribed EEC. If UE's location information is not available, the ECS may obtain the UE location by utilizing the capabilities of the 3GPP core network as specified in clause 8.10.2. If AC profile(s) were provided by the EEC during subscription creation, the ECS identifies the EES(s) based on the provided AC profile(s) and the UE location. If AC profiles(s) were not provided, then:
 - if available, the ECS identifies the EES(s) based on the UE-specific service information at the ECS and the UE location;
 - ECS identifies the EES(s) by applying the ECSP policy (e.g. based only on the UE location);

NOTE 1: Details of the UE-specific service information and how it is available at the ECS is out of scope.

NOTE 2: Both steps are evaluated prior to sending a response.

The ECS also determines other information that needs to be provisioned, e.g. identification of the EDN, EDN service area, EES endpoints.

2. The ECS sends a provisioning notification to the EEC with the list of EDN configuration information determined in step 1.

If the EDN configuration information in the service provisioning notification includes an LADN DNN as an identifier for the EDN, the EEC considers the LADN as the EDN. Therefore, the service area of EDN is the LADN Service Area, which can be discovered using the UE Registration Procedure.

If the ECS provided information regarding the service continuity support of individual EESs, the EEC may take this information into account when selecting an EES for EEC registration, EAS discovery or T-EAS discovery, respectively.

NOTE 3: Even after the EEC establishes a connection to the EES using information received in step 2, the EES can issue AF request to influence traffic routing from EEC to EES as specified in 3GPP TS 23.501 [2] clause 5.6.7.

8.3.3.2.3.4 Subscription update

Figure 8.3.3.2.3.4-1 illustrates the service provisioning subscription update procedure between the EEC and the ECS.

Pre-conditions:

1. The EEC has subscribed with the ECS for the provisioning information as specified in clause 8.3.3.2.3.2.

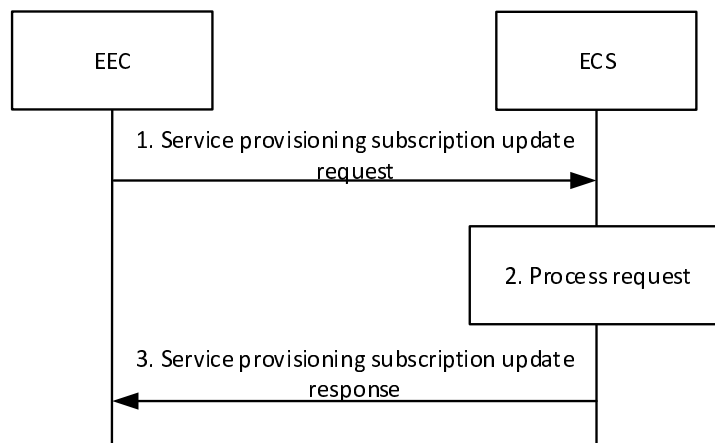


Figure 8.3.3.2.3.4-1: Service provisioning subscription update

1. The EEC sends a service provisioning subscription update request to the ECS. The service provisioning subscription update request includes the security credentials of the EEC received during EEC authorization procedure along with the subscription identifier and may include the UE identifier such as GPSI, connectivity information, proposed expiration time for the updated subscription and AC profile(s).
2. Upon receiving the request, the ECS performs an authorization check to verify whether the EEC has authorization to perform the operation. If required, the ECS may utilize the capabilities (e.g. UE location) of the 3GPP core network as specified in clause 8.10.2. If authorized, the ECS updates the stored subscription for provisioning as requested in step 1.
3. The ECS responds with a service provisioning subscription update response, which may include the expiration time, indicating when the updated subscription will automatically expire. To maintain the subscription, the EEC shall send a Service provisioning subscription update request prior to the expiration time. If a Service provisioning subscription update request is not received prior to the expiration time, the ECS shall treat the EEC as implicitly unsubscribed.

8.3.3.2.3.5 Unsubscribe

Figure 8.3.3.2.3.5-1 illustrates the service provisioning unsubscribe procedure between the EEC and the ECS.

Pre-conditions:

1. The EEC has subscribed with the ECS for the provisioning information as specified in clause 8.3.3.2.3.2.

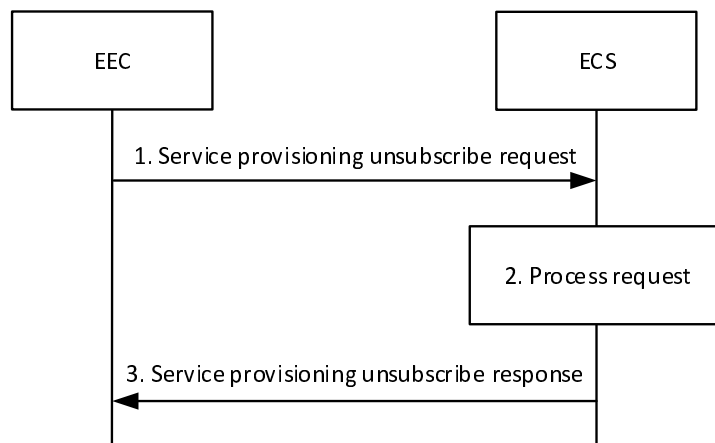


Figure 8.3.3.2.3.5-1: Service provisioning unsubscribe

1. The EEC sends a service provisioning unsubscribe request to the ECS. The service provisioning unsubscribe request includes the security credentials of the EEC received during EEC authorization procedure along with the subscription identifier.
2. Upon receiving the request, the ECS performs an authorization check to verify whether the EEC has authorization to perform the operation. If authorized, the ECS cancels the subscription for provisioning as requested in step 1.
3. The ECS responds with a service provisioning unsubscribe response.

8.3.3.3 Information flows

8.3.3.3.1 General

The following information flows are specified for service provisioning:

- Service provisioning request and response;
- Service provisioning subscription request and response;
- Service provisioning notification;
- Service provisioning update request and response; and
- Service provisioning unsubscribe request and response.

8.3.3.3.2 Service provisioning request

Table 8.3.3.3.2-1 describes the information elements for service provisioning request from the EEC to the ECS.

Table 8.3.3.3.2-1: Service provisioning request

Information element	Status	Description
EECID	M	Unique identifier of the EEC.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
AC Profile(s)	O	Information about services the EEC wants to connect to, as described in Table 8.2.2-1.
EEC Service Continuity Support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC.
UE Identifier	O	The identifier of the UE (i.e. GPSI or identity token)
Connectivity information	O	List of connectivity information for the UE, e.g. PLMN ID, SSID.
UE location	O	The location information of the UE. The UE location is described in clause 7.3.2.

Editor's Note: [SA3] Whether the EECID and the UE ID included in request of EDGE-1 & 4 interactions is part of the security credential is SA3's responsibility.

8.3.3.3.3 Service provisioning response

Table 8.3.3.3.3-1 describes the information elements for service provisioning response from the ECS to the EEC.

Table 8.3.3.3.3-1: Service provisioning response

Information element	Status	Description
Successful response	O	Indicates that the service provisioning request was successful.
> List of EDN configuration information	M	List of EDN configuration information as defined in Table 8.3.3.3.3-2.
Failure response	O	Indicates that the service provisioning request failed.
> Cause	O	Indicates the cause of service provisioning request failure.

Table 8.3.3.3.3-2: EDN configuration information

Information element	Status	Description
EDN connection information (NOTE 1)	M	Information required by the UE to establish connection with the EDN.
> DNN/APN	M	Data Network Name/Access Point Name
> S-NSSAI	O	Network Slice information
> EDN Topological Service Area	O	The EDN serves UEs that are connected to the Core Network from one of the cells included in this service area. See possible formats in Table 8.2.7-1.
List of EESs	M	List of EESs of the EDN.
> EESID	M	The identifier of the EES
> EES Endpoint	M	The endpoint address (e.g. URI, IP address) of the EES
> EASIDs (NOTE 2)	O	List of EASIDs registered with the EES.
> EES Provider identifier	O	The identifier of the EES Provider (such as ECSP)
> EES Topological Service Area	O	The EES serves UEs that are connected to the Core Network from one of the cells included in this service area. EECs in UEs that are located outside this area shall not be served. See possible formats in Table 8.2.7-1.
> EES Geographical Service Area	O	The area being served by the EES in Geographical values (as specified in clause 7.3.3.3)
> List of EES DNAI(s)	O	DNAI(s) associated with the EES/EAS. This IE is used as Potential Locations of Applications in clause 5.6.7 of 3GPP TS 23.501 [2].
> EES Service continuity support	O	Indicates if the EES supports service continuity or not. This IE also indicates which ACR scenarios are supported by the EES.
> EEC registration configuration	M	Indicates whether the EEC is required to register on the EES to use edge services or not.
> Security Credential	O	Indicates the security credential sent by the ECS. The security credential is used by EEC to communicate with the EES as specified in 3GPP TS 33.558 [23], clause 6.2.
Lifetime	O	Time duration for which the EDN configuration information is valid and supposed to be cached in the EEC.
NOTE 1: If the UE is provisioned or pre-configured with URSP rules by the HPLMN, the UE handles the precedence between EDN connection info and URSP rules as defined in 3GPP TS 23.503 [12] clause 6.1.2.2.1. EDN connection info is considered to be part of UE Local Configurations.		
NOTE 2: EAS information is limited to the EEC requested applications. If no AC profiles were present in the service provisioning request, the EAS information is subject to the ECSP policy (e.g. no EAS information or a subset of EAS information related to the EES).		

8.3.3.3.4 Service provisioning subscription request

Table 8.3.3.3.4-1 describes the information elements for service provisioning subscription request from the EEC to the ECS.

Table 8.3.3.3.4-1: Service provisioning subscription request

Information element	Status	Description
EECID	M	Unique identifier of the EEC.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
Notification Target Address	O	The Notification Target Address (e.g. URL) where the notifications destined for the EEC should be sent to.
AC profile(s)	O	Information about services the EEC wants to connect to, as described in Table 8.2.2-1.
EEC Service Continuity Support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC.
UE Identifier	O	The identifier of the UE (i.e. GPSI or identity token)
Connectivity information	O	List of connectivity information for the UE, e.g. PLMN ID, SSID.
Proposed expiration time	O	Proposed expiration time for the subscription

8.3.3.3.5 Service provisioning subscription response

Table 8.3.3.3.5-1 describes the information elements for service provisioning subscription response from the ECS to the EEC.

Table 8.3.3.3.5-1: Service provisioning subscription response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.3.3.3.6 Service provisioning notification

Table 8.3.3.3.6-1 describes the information elements for service provisioning notification from the ECS to the EEC.

Table 8.3.3.3.6-1: Service provisioning notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the ECS for the request
List of EDN configuration information	M	List of EDN configuration information as defined in Table 8.3.3.3.3-2.

8.3.3.3.7 Service provisioning subscription update request

Table 8.3.3.3.7-1 describes the information elements for service provisioning subscription update request from the EEC to the ECS.

Table 8.3.3.3.7-1: Service provisioning subscription update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be updated
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
Connectivity information	O	List of connectivity information for the UE, e.g. PLMN ID, SSID.
Proposed expiration time	O	Proposed expiration time for the subscription
AC profile(s)	O	Information about services the EEC wants to connect to, as described in Table 8.2.2-1.
EEC Service Continuity Support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC.

8.3.3.3.8 Service provisioning subscription update response

Table 8.3.3.3.8-1 describes the information elements for service provisioning subscription update response from the ECS to the EEC.

Table 8.3.3.3.8-1: Service provisioning subscription update response

Information element	Status	Description
Successful response	O	Indicates that the subscription update request was successful.
> Expiration time	O	Indicates the expiration time of the updated subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription update request failed.
> Cause	O	Indicates the cause of subscription update request failure

8.3.3.3.9 Service provisioning unsubscribe request

Table 8.3.3.3.9-1 describes the information elements for service provisioning unsubscribe request from the EEC to the ECS.

Table 8.3.3.3.9-1: Service provisioning unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the ECS
Security credentials	M	Security credentials of the EEC

8.3.3.3.10 Service provisioning unsubscribe response

Table 8.3.3.3.10-1 describes the information elements for service provisioning unsubscribe response from the ECS to the EEC.

Table 8.3.3.3.10-1: Service provisioning unsubscribe response

Information element	Status	Description
Successful response	O	Indicates that the unsubscribe request was successful.
Failure response	O	Indicates that the unsubscribe request failed.
> Cause	O	Indicates the cause of unsubscribe request failure

8.3.3.4 APIs

8.3.3.4.1 General

Table 8.3.3.4.1-1 illustrates the API for service provisioning.

Table 8.3.3.4.1-1: Eecs_ServiceProvisioning API

API Name	API Operations	Operation Semantics	Consumer(s)
Eecs_ServiceProvisioning	Request	Request/Response	EEC
	Subscribe	Subscribe/Notify	EEC
	Notify		
	UpdateSubscription		
	Unsubscribe		

8.3.3.4.2 Eecs_ServiceProvisioning_Request operation

API operation name: Eecs_ServiceProvisioning_Request

Description: The consumer requests for one time service provisioning information.

Inputs: See clause 8.3.3.3.2.

Outputs: See clause 8.3.3.3.3.

See clause 8.3.3.2.2 for details of usage of this operation.

8.3.3.4.3 Eecs_ServiceProvisioning_Subscribe operation

API operation name: Eecs_ServiceProvisioning_Subscribe

Description: The consumer subscribes for service provisioning information.

Inputs: See clause 8.3.3.3.4.

Outputs: See clause 8.3.3.3.5.

See clause 8.3.3.2.3.2 for details of usage of this operation.

8.3.3.4.4 Eecs_ServiceProvisioning_Notify operation

API operation name: Eecs_ServiceProvisioning_Notify

Description: The consumer is notified with service provisioning information.

Inputs: See clause 8.3.3.3.6.

Outputs: None.

See clause 8.3.3.2.3.3 for details of usage of this operation.

8.3.3.4.5 Eecs_ServiceProvisioning_UpdateSubscription operation

API operation name: Eecs_ServiceProvisioning_UpdateSubscription

Description: The consumer updates an existing subscription for service provisioning information.

Inputs: See clause 8.3.3.3.7.

Outputs: See clause 8.3.3.3.8.

See clause 8.3.3.2.3.4 for details of usage of this operation.

8.3.3.4.6 Eecs_ServiceProvisioning_Unsubscribe operation

API operation name: Eecs_ServiceProvisioning_Unsubscribe

Description: The consumer cancels an existing subscription for service provisioning information.

Inputs: See clause 8.3.3.3.9.

Outputs: See clause 8.3.3.3.10.

See clause 8.3.3.2.3.5 for details of usage of this operation.

8.4 Registration

8.4.1 General

Registration procedures allow entities in the edge deployment to deliver information to other entities.

The following registrations are supported:

- EEC registration with EES;
- EAS registration with EES; and
- EES registration with ECS.

8.4.2 EEC Registration

8.4.2.1 General

An EEC performs registration with an EES in order to provide information that can be used by the EES in Edge Computing services. The procedure also enables initialization, update and removal of the EEC context information at the EES. The context may be further used for edge-specific operations or processing, e.g. analytics.

An EEC may be registered with one or more EESs on behalf of one or more ACs simultaneously.

8.4.2.2 Procedures

8.4.2.2.1 General

Following are supported for EEC registration:

- EEC registration procedure;
- EEC registration update procedure;
- EEC de-registration procedure; and
- EEC Context relocation procedure.

NOTE: In this version of specification, each registration procedure provides for registering a single EEC per UE.

8.4.2.2.2 EEC registration

Figure 8.4.2.2.2-1 illustrates EEC registration procedure.

Pre-conditions:

1. The EEC is authorized to access the EES for the purpose of performing registration and has received relevant security credentials as specified in clause 8.11; and

2. The EEC has received service provisioning information from the ECS, including information for accessing the EES.

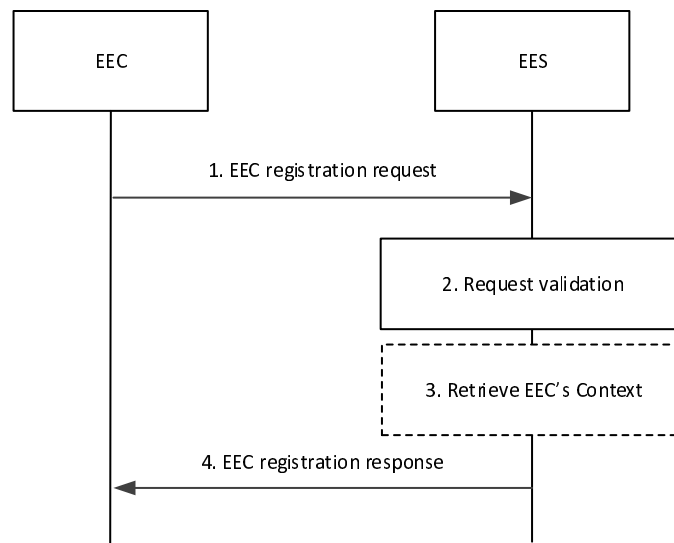


Figure 8.4.2.2-1: EEC registration procedure

1. The EEC sends EEC registration request to the EES. The request from the client includes the security credentials received after successful authorization for edge computing services and may include a proposed expiration time. The request also optionally includes information indicating to the EES how the EEC expects to use the services of the EES.

If the EEC is moving to this EES from the purview of another EES, called S-EES, the request from the EEC may include the identity and endpoint of the S-EES and an EEC context ID that was provided by the S-EES to maintain continuity of the EEC context and to authorize EEC context relocation. If the EEC registration is being performed as part of ACR, the EEC shall not include the S-EES endpoint and the EEC context ID.

2. Upon receiving the request from the EEC, the EES validates the registration request and verifies the security credentials. The EES further determines whether the requirements that were indicated in the AC Profile(s) can be fulfilled and reserves corresponding resources.

NOTE: Resource reservation at EEC registration ensures that the EES provides services for the duration of the registration.

3. Upon successful validation of the request, if the received EEC registration request contains an EEC context ID and a S-EES Endpoint, the EES performs a EEC Context Pull relocation (clause 8.9.2.2) from the S-EES. The source and target EES perform EEC Context handling as detailed in clause 8.9.1.

NOTE 1: Only a single EEC Context ID may be provided in the EEC registration request.

NOTE 2: In this version of specification, each registration procedure relocates a single EEC context.

NOTE 3: Step 3 is executed when EEC determines to change its connection from S-EES to T-EES and ACR is not required.

If the EEC registration request fails after the EEC Context Pull relocation, e.g., the EES cannot reserve the necessary resources while meeting the capability requirements of the existing registered EECs, the EES shall determine the EEC Context information stale and send a failure response with a corresponding cause.

4. The EES sends a successful EEC registration response, which includes the registration ID and may include a newly assigned EEC context ID. If the EEC registration request contains AC Profile(s), and the EES determines that the requirements indicated in the AC profile(s) cannot be fulfilled for some of the AC profile(s), the EES shall include the list of ACIDs of such AC Profile(s) and may include appropriate reasons. If step 3 was executed, the EEC registration response also includes EEC context retrieval result. The EEC stores the new EEC

context ID and uses it if and when it registers with another EES. The EES may also provide an expiration time to indicate to the EEC when the registration will automatically expire. To maintain the registration, the EEC shall send a registration update request prior to the expiration. If a registration update request is not received prior to the expiration time, the EES shall treat the EEC as implicitly de-registered.

If the EEC context relocation status indicates that the EEC context relocation was not successful, then the EEC performs the required EDGE-1 subscriptions at the T-EES.

8.4.2.2.3 EEC registration update

Figure 8.4.2.2.3-1 illustrates EEC registration update procedure.

Pre-conditions:

1. EEC has already registered with the EES.

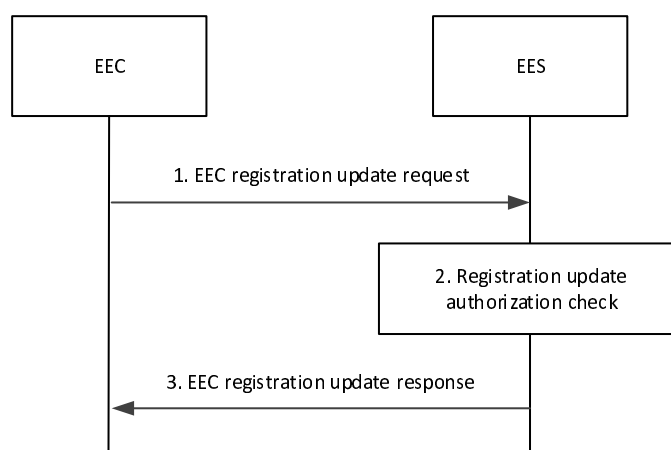


Figure 8.4.2.2.3-1: EEC registration update procedure

1. The EEC sends EEC registration update request to the EES. The request from the client includes the security credentials received after successful authorization for edge computing services and may include a proposed expiration time and AC profile(s).
2. Upon receiving the request from the EEC, the EES validates the registration update request and verifies the security credentials.
3. Upon successful validation of the request, the EES sends a successful registration update response, which may include updated expiration time to indicate to the EEC when the updated registration will automatically expire. If the EEC registration update request contains AC Profile(s), and the EES determines that the requirements indicated in the AC profile(s) cannot be fulfilled for some of the AC profile(s), the EES shall include the list of ACIDs of such AC Profile(s) and may include appropriate reasons. To maintain the registration, the EEC shall send a registration update request prior to the expiration time. If a registration update request is not received prior to the expiration time, the EES shall treat the EEC as implicitly de-registered.

8.4.2.2.4 EEC de-registration

Figure 8.4.2.2.4-1 illustrates EEC de-registration procedure.

Pre-conditions:

1. EEC has already registered with the EES.

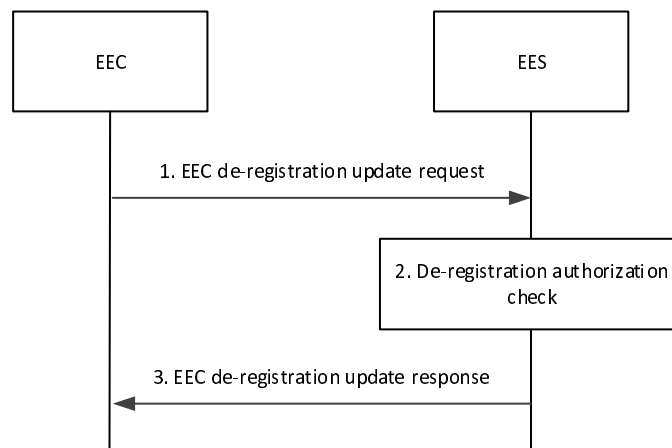


Figure 8.4.2.2.4-1: EEC de-registration procedure

1. The EEC sends EEC de-registration request to the EES. The request from the client includes the security credentials received after successful authorization for edge computing services.
2. Upon receiving the request from the EEC, the EES validates the de-registration request and verifies the security credentials.
3. Upon successful authorization, the EES sends a successful de-registration response.

8.4.2.3 Information flows

8.4.2.3.1 General

The following information flows are specified for EEC registration:

- EEC registration request and response;
- EEC registration update request and response; and
- EEC registration de-registration request and response.

8.4.2.3.2 EEC registration request

Table 8.4.2.3.2-1 describes information elements in the EEC registration request from the EEC to the EES.

Table 8.4.2.3.2-1: EEC registration request

Information element	Status	Description
EECID	M	Unique identifier of the EEC.
UE Identifier	O	The identifier of the hosting UE (i.e. GPSI or identity token)
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
AC Profile(s)	O	Profiles of ACs for which the EEC provides edge enabling services. AC Profiles are further described in Table 8.2.2-1.
EEC Service Continuity Support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC.
Proposed expiration time	O	Proposed expiration time for the registration.
EEC context ID (NOTE)	O	Identifier of the EEC context obtained from a previous registration.
Source EESID (NOTE)	O	Identifier of the EES that provided EEC context ID.
Source EES Endpoint (NOTE)	O	The endpoint address (e.g. URI, IP address) of the EES that provided EEC context ID.
NOTE: This IE shall not be present when EEC registration is performed as part of ACR.		

8.4.2.3.3 EEC registration response

Table 8.4.2.3.3-1 describes information elements in the EEC registration response from the EES to the EEC.

Table 8.4.2.3.3-1: EEC registration response

Information element	Status	Description
Successful response	O	Indicates that the registration request was successful.
> Registration ID	M	Identifier of the EEC registration.
> Expiration time	M	Indicates the expiration time of the registration. To maintain an active registration status, a registration update is required before the expiration time.
> EEC context ID	O	Identifier of the EEC Context information available at the EES that performed the registration.
> EEC Context Relocation status	O	Indicates whether the EEC context retrieval from the S-EES was successful or not.
> list of unfulfilled AC information	O	List of ACIDs of the AC Profile(s) for which the requirements indicated in the AC profile(s) cannot be fulfilled
>> ACID	M	Application Identifier
>> reason	O	Reason indicating the cause (e.g. EAS not available, requirements cannot be fulfilled)
Failure response	O	Indicates that the registration request failed.
> Cause	M	Provides the cause for registration request failure.

8.4.2.3.4 EEC registration update request

Table 8.4.2.3.4-1 describes information elements in the EEC registration update request from the EEC to the EES.

Table 8.4.2.3.4-1: EEC registration update request

Information element	Status	Description
Registration ID	M	Identifier of the EEC registration.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
AC profile(s)	O	AC Profile as described in Table 8.2.2-1
Proposed expiration time	O	Proposed expiration time for the updated registration.

8.4.2.3.5 EEC registration update response

Table 8.4.2.3.5-1 describes information elements in the EEC registration update response from the EES to the EEC.

Table 8.4.2.3.5-1: EEC registration update response

Information element	Status	Description
Successful response	O	Indicates that the registration update request was successful.
> Expiration time	M	Indicates the expiration time of the registration. To maintain an active registration status, a registration update is required before the expiration time.
> list of unfulfilled AC information	O	List of ACIDs of the AC Profile(s) for which the requirements indicated in the AC profile(s) cannot be fulfilled
>> ACID	M	Application Identifier
>> reason	O	Reason indicating the cause (e.g. EAS not available, requirements cannot be fulfilled)
Failure response	O	Indicates that the registration update request failed.

8.4.2.3.6 EEC de-registration request

Table 8.4.2.3.6-1 describes information elements in the EEC de-registration request from the EEC to the EES.

Table 8.4.2.3.6-1: EEC de-registration request

Information element	Status	Description
Registration ID	M	Identifier of the EEC registration.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.

8.4.2.3.7 EEC de-registration response

Table 8.4.2.3.7-1 describes information elements in the EEC de-registration response from the EES to the EEC.

Table 8.4.2.3.7-1: EEC registration update response

Information element	Status	Description
Successful response	O	Indicates that the de-registration request was successful.
Failure response	O	Indicates that the de-registration request failed.
> Cause	M	Provide the cause for de-registration request failure.

8.4.2.4 APIs

8.4.2.4.1 General

Table 8.4.2.4.1-1 illustrates the API for EEC registration.

Table 8.4.2.4.1-1: Eees_EECRegistration API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_EECRegistration	Request	Request/Response	EEC
	Update		
	Deregister		

8.4.2.4.2 Eees_EECRegistration_Request operation

API operation name: Eees_EECRegistration_Request

Description: The consumer requests to register the EEC on the EES.

Inputs: See clause 8.4.2.3.2.

Outputs: See clause 8.4.2.3.3.

See clause 8.4.2.2.2 for details of usage of this operation.

8.4.2.4.3 Eees_EECRegistration_Update operation

API operation name: Eees_EECRegistration_Update

Description: The consumer requests to update the registered information of the EEC on the EES.

Inputs: See clause 8.4.2.3.4.

Outputs: See clause 8.4.2.3.5.

See clause 8.4.2.2.3 for details of usage of this operation.

8.4.2.4.4 Eees_EECRegistration_Deregister operation

API operation name: Eees_EECRegistration_Deregister

Description: The consumer requests to de-register the EEC from the EES.

Inputs: See clause 8.4.2.3.6.

Outputs: See clause 8.4.2.3.7.

See clause 8.4.2.2.4 for details of usage of this operation.

8.4.3 EAS Registration

8.4.3.1 General

The EAS Registration procedure allows an EAS to provide its information to an EES in order to enable its discovery.

If there is a change in the requirements or the information of an EAS, it uses the EAS registration update procedure to update the EES.

The EAS uses the EAS de-registration procedure to remove its information from the EES.

EAS registration at the EES can be time bound. So, to maintain the registration, the EAS needs to send a registration update request prior to the registration expiration time. If a registration update request is not received prior to the registration expiration time, the EES treats the EAS as implicitly de-registered.

8.4.3.2 Procedures

8.4.3.2.1 General

Following are supported for EAS registration:

- EAS registration procedure;
- EAS registration update procedure; and
- EAS de-registration procedure.

8.4.3.2.2 EAS registration

Pre-conditions:

1. The EAS has been configured with an EASID;
2. The EAS has been configured with the address (e.g. URI) of the EES; and
3. Both the EAS and EES have the necessary credentials to enable communications.

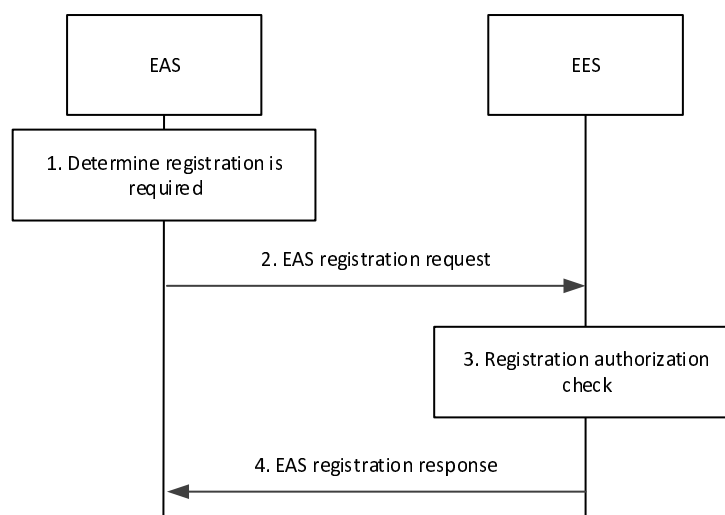


Figure 8.4.3.2.2-1: EAS Registration procedure

1. The EAS determines that registration to the EES is needed (e.g. the EAS is instantiated and started up).

2. The EAS sends an EAS registration request to the EES. The request shall include the EAS profile and may include proposed expiration time for the registration.
3. The EES performs an authorization check to verify whether the EAS has the authorization to register on the EES.
4. Upon successful authorization, the EES stores the EAS Profile for later use (e.g. for serving EAS discovery requests received from EECs, etc.) and replies to the EAS with an EAS registration response. The EES may provide an expiration time to indicate to the EAS when the registration will automatically expire. To maintain the registration, the EAS shall send a registration update request prior to the expiration time. If a registration update request is not received prior to the expiration time, the EES shall treat the EAS as implicitly de-registered.

8.4.3.2.3 EAS registration update

Pre-conditions:

1. The EAS has already registered with the EES.

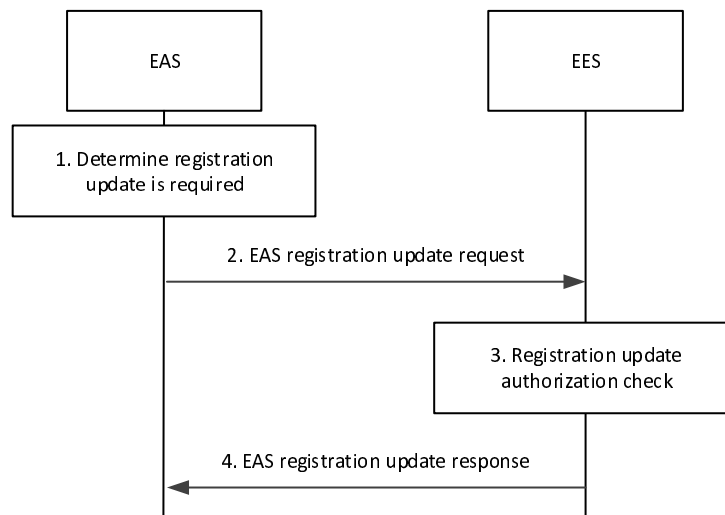


Figure 8.4.3.2.3-1: EAS registration update procedure

1. The EAS determines that its existing registration needs to be updated (e.g. because the EAS's status or availability schedule has changed, or EAS's registration is about to expire).
2. The EAS sends an EAS registration update request to the EES. The request shall include the registration ID and may include the EAS profile and proposed expiration time for the updated registration.
3. The EES performs an authorization check to verify whether the EAS has the authorization to update the registration on the EES.
4. Upon successful authorization, the EES updates the registered EAS Profile and replies to the EAS with an EAS registration update response. The EES may provide an updated expiration time to indicate to the EAS when the updated registration will automatically expire. To maintain the registration, the EAS shall send a registration update request prior to the expiration time. If a registration update request is not received prior to the expiration time, the EES shall treat the EAS as implicitly de-registered.

8.4.3.2.4 EAS de-registration

Pre-conditions:

1. The EAS has already registered with the EES.

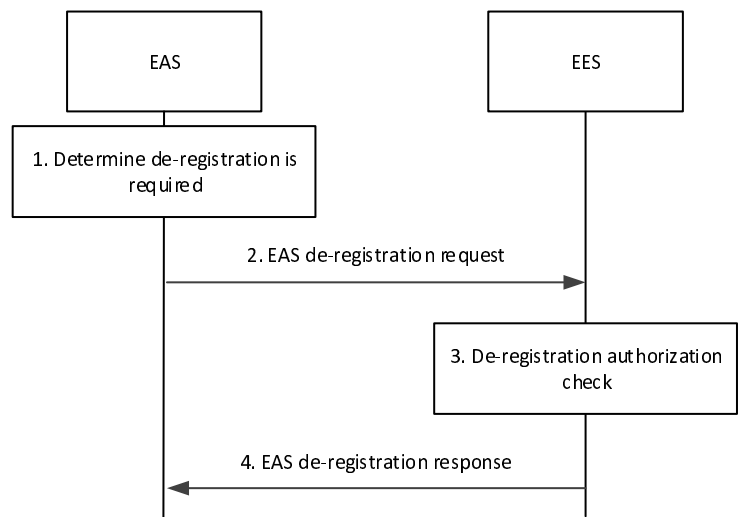


Figure 8.4.3.2.4-1: EAS de-registration procedure

1. The EAS determines that its existing registration needs to be terminated (e.g. because the services of the EAS are not needed anymore).
2. The EAS sends an EAS de-registration request to the EES. The request shall include the registration ID.
3. The EES performs an authorization check to verify whether the EAS has the authorization to de-register explicitly.
4. Upon successful authorization, the EES removes the registered EAS Profile and replies to the EAS with an EAS de-registration response.

8.4.3.3 Information flows

8.4.3.3.1 General

The following information flows are specified for EAS registration:

- EAS registration request and response;
- EAS registration update request and response; and
- EAS registration de-registration request and response.

8.4.3.3.2 EAS registration request

Table 8.4.3.3.1-2 describes information elements in the EAS registration request from the EAS to the EES.

Table 8.4.3.3.2-1: EAS registration request

Information element	Status	Description
EAS Profile	M	EAS Profile as described in Table 8.2.4-1
Security credentials	M	Security credentials of the EAS.
Proposed expiration time	O	Proposed expiration time for the registration

8.4.3.3.3 EAS registration response

Table 8.4.3.3.3-1 describes information elements in the EAS registration response from the EES to the EAS.

Table 8.4.3.3.3-1: EAS registration response

Information element	Status	Description
Successful response	O	Indicates that the registration request was successful.
> Registration ID	M	Identifier of the registration.
> Expiration time	O	Indicates the expiration time of the registration. To maintain an active registration status, a registration update is required before the expiration time. If the Expiration time IE is not included, it indicates that the registration never expires.
Failure response	O	Indicates that the registration request failed.
> Cause	O	Indicates the cause of registration request failure

8.4.3.3.4 EAS registration update request

Table 8.4.3.3.4-1 describes information elements in the EAS registration update request from the EAS to the EES.

Table 8.4.3.3.4-1: EAS registration update request

Information element	Status	Description
Registration ID	M	Identifier of the registration.
Security credentials	M	Security credentials of the EAS
Updated EAS Profile (NOTE)	O	EAS Profile as described in Table 8.2.4-1 with updated information. Included only if there is an update in EAS information.
Proposed expiration time (NOTE)	O	Proposed expiration time for the registration
NOTE: At least one of the IEs is included.		

8.4.3.3.5 EAS registration update response

Table 8.4.3.3.5-1 describes information elements in the EAS registration update response from the EES to the EAS.

Table 8.4.3.3.5-1: EAS registration update response

Information element	Status	Description
Successful response	O	Indicates that the registration update request was successful.
> Expiration time	O	Indicates the expiration time of the updated registration. To maintain an active registration status, a registration update is required before the expiration time. If the Expiration time IE is not included, it indicates that the updated registration never expires.
Failure response	O	Indicates that the registration update request failed.
> Cause	O	Indicates the cause of registration update request failure

8.4.3.3.6 EAS de-registration request

Table 8.4.3.3.6-1 describes information elements in the EAS de-registration request from the EAS to the EES.

Table 8.4.3.3.6-1: EAS de-registration request

Information element	Status	Description
Registration ID	M	Identifier of the registration.
Security credentials	M	Security credentials of the EAS

8.4.3.3.7 EAS de-registration response

Table 8.4.3.3.7-1 describes information elements in the EAS de-registration response from the EES to the EAS.

Table 8.4.3.3.7-1: EAS de-registration response

Information element	Status	Description
Successful response	O	Indicates that the de-registration request was successful.
Failure response	O	Indicates that the de-registration request failed.
> Cause	O	Indicates the cause of de-registration request failure

8.4.3.4 APIs

8.4.3.4.1 General

Table 8.4.3.4.1-1 illustrates the API for EAS registration.

Table 8.4.3.4.1-1: Eees_EASRegistration API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_EASRegistration	Request	Request/Response	EAS
	Update		
	Deregister		

8.4.3.4.2 Eees_EASRegistration_Request operation

API operation name: Eees_EASRegistration_Request

Description: The consumer requests to register the EAS on the EES.

Inputs: See clause 8.4.3.3.2.

Outputs: See clause 8.4.3.3.3.

See clause 8.4.3.2.2 for details of usage of this operation.

8.4.3.4.3 Eees_EASRegistration_Update operation

API operation name: Eees_EASRegistration_Update

Description: The consumer requests to update the registered information of the EAS on the EES.

Inputs: See clause 8.4.3.3.4.

Outputs: See clause 8.4.3.3.5.

See clause 8.4.3.2.3 for details of usage of this operation.

8.4.3.4.4 Eees_EASRegistration_Deregister operation

API operation name: Eees_EASRegistration_Deregister

Description: The consumer requests to deregister the EAS from the EES.

Inputs: See clause 8.4.3.3.6.

Outputs: See clause 8.4.3.3.7.

See clause 8.4.3.2.4 for details of usage of this operation.

8.4.4 EES Registration

8.4.4.1 General

The EES Registration procedure allows an EES to provide information to an ECS in order to enable provisioning EES(s) to an EEC.

The EES registration update procedure allows an EES to update the ECS, if there is a change in the information at the EES.

The EES uses the EES de-registration procedure to remove its information from the ECS.

8.4.4.2 Procedures

8.4.4.2.1 General

8.4.4.2.2 EES registration

Pre-conditions:

1. The EES has the address (e.g. URI) of the ECS;
2. Both, the EES and ECS, have the necessary credentials to enable communications.

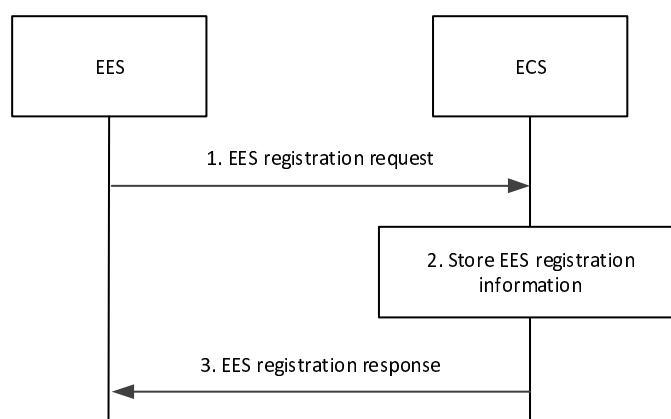


Figure 8.4.4.2.2-1: EES Registration procedure

1. The EES sends the EES registration request to the ECS. The request from the EES includes the EES profile and EES security credentials. The request may include a proposed expiration time for the registration.
2. Upon receiving the request from the EES, the ECS verifies the security credentials of the EES and stores the EES registration information obtained in step 1.
3. The ECS sends an EES registration response indicating success or failure of the registration operation. The ECS may provide an updated expiration time to indicate to the EES when the registration will automatically expire. To maintain the registration, the EES shall send a registration update request prior to the expiration time. If a registration update request is not received prior to the expiration time, the ECS shall treat the EES as implicitly de-registered.

8.4.4.2.3 EES registration update

Pre-conditions:

1. The EES has already registered on the ECS.

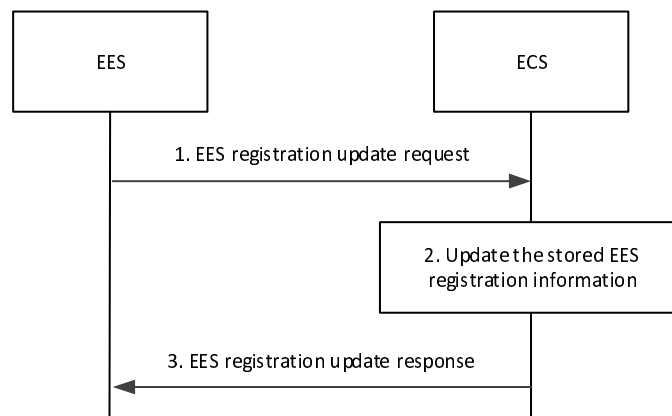


Figure 8.4.4.2.3-1: EES registration update procedure

1. The EES sends the EES registration update request to the ECS. The request from the EES includes the registration identity and EES security credentials, and may include proposed expiration time and updated EES profile.
2. Upon receiving the request from the EES, the ECS verifies the security credentials of the EES and stores the updated EES registration information obtained in step 1.
3. The ECS sends an EES registration update response indicating success or failure of the registration update operation. The ECS may provide an updated expiration time to indicate to the EES when the updated registration will automatically expire. To maintain the registration, the EES shall send a registration update request prior to the expiration time. If a registration update request is not received prior to the expiration time, the ECS shall treat the EES as implicitly de-registered.

8.4.4.2.4 EES de-registration

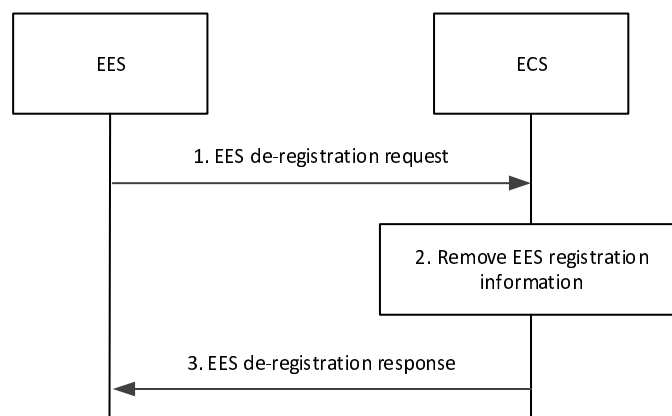


Figure 8.4.4.2.4-1: EES de-registration procedure

1. The EES sends the EES de-registration request to the ECS. The request from the EES includes the registration identity and EES security credentials.
2. Upon receiving the request from the EES, the ECS verifies the security credentials of the EES and removes the corresponding EES registration information.
3. The ECS sends an EES de-registration response indicating success or failure of the de-registration operation.

8.4.4.3 Information elements

8.4.4.3.1 General

The following information flows are specified for EES registration:

- EES registration request and response;
- EES registration update request and response; and
- EES registration de-registration request and response.

8.4.4.3.2 EES registration request

Table 8.4.4.3.2-1 describes information elements for an EES registration request from the EES to the ECS.

Table 8.4.4.3.2-1: EES registration request

Information element	Status	Description
EES Profile	M	Profile information as specified in Table 8.2.6-1
Security credentials	M	Security credentials of the EES.
Proposed expiration time	O	Proposed expiration time for the registration

8.4.4.3.3 EES registration response

Table 8.4.4.3.3-1 describes information elements for an EES registration response from the ECS to the EES.

Table 8.4.4.3.3-1: EES registration response

Information element	Status	Description
Successful response	O	Indicates that the registration request was successful.
> Registration ID	M	Identifier of the registration.
> Expiration time	O	Indicates the expiration time of the registration. To maintain an active registration status, a registration update is required before the expiration time. If the Expiration time IE is not included, it indicates that the registration never expires.
Failure response	O	Indicates that the registration request failed.
> Cause	O	Indicates the cause of registration request failure

8.4.4.3.4 EES registration update request

Table 8.4.4.3.4-1 describes information elements for an EES registration update request from the EES to the ECS.

Table 8.4.4.3.4-1: EES registration update request

Information element	Status	Description
Updated EES Profile (NOTE)	O	Profile information as specified in Table 8.2.6-1
Security credentials	M	Security credentials of the EES.
Registration ID	M	Identifier of the registration.
Proposed expiration time (NOTE)	O	Proposed expiration time for the registration
NOTE: At least one of the IEs is included.		

8.4.4.3.5 EES registration update response

Table 8.4.4.3.5-1 describes information elements for an EES registration update response from the ECS to the EES.

Table 8.4.4.3.5-1: EES registration update response

Information element	Status	Description
Successful response	O	Indicates that the registration update request was successful.
> Expiration time	O	Indicates the expiration time of the updated registration. To maintain an active registration status, a registration update is required before the expiration time. If the Expiration time IE is not included, it indicates that the updated registration never expires.
Failure response	O	Indicates that the registration update request failed.
> Cause	O	Indicates the cause of registration update request failure

8.4.4.3.6 EES de-registration request

Table 8.4.4.3.6-1 describes information elements for an EES de-registration request from the EES to the ECS.

Table 8.4.4.3.6-1: EES de-registration request

Information element	Status	Description
Registration ID	M	Identifier of the registration.
Security credentials	M	Security credentials of the EES

8.4.4.3.7 EES de-registration response

Table 8.4.4.3.7-1 describes information elements for an EES de-registration response from the ECS to the EES.

Table 8.4.4.3.7-1: EES de-registration response

Information element	Status	Description
Successful response	O	Indicates that the de-registration request was successful.
Failure response	O	Indicates that the de-registration request failed.
> Cause	O	Indicates the cause of de-registration request failure

8.4.4.4 APIs

8.4.4.4.1 General

Table 8.4.4.4.1-1 illustrates the API for EES registration.

Table 8.4.4.4.1-1: Eecs_EESRegistration API

API Name	API Operations	Operation Semantics	Consumer(s)
Eecs_EESRegistration	Request	Request/Response	EES
	Update		
	Deregister		

8.4.4.4.2 Eecs_EESRegistration_Request operation

API operation name: Eecs_EESRegistration_Request

Description: The consumer requests to register the EES on the ECS.

Inputs: See clause 8.4.4.3.2.

Outputs: See clause 8.4.4.3.3.

See clause 8.4.4.2.2 for details of usage of this operation.

8.4.4.4.3 Eecs_EESRegistration_Update operation

API operation name: Eecs_EESRegistration_Update

Description: The consumer requests to update the registered information of the EES on the ECS.

Inputs: See clause 8.4.4.3.4.

Outputs: See clause 8.4.4.3.5.

See clause 8.4.4.2.3 for details of usage of this operation.

8.4.4.4.4 Eecs_EESRegistration_Deregister operation

API operation name: Eecs_EESRegistration_Deregister

Description: The consumer requests to deregister the EES from the ECS.

Inputs: See clause 8.4.4.3.6.

Outputs: See clause 8.4.4.3.7.

See clause 8.4.4.2.4 for details of usage of this operation.

8.5 EAS discovery

8.5.1 General

Discovery procedures enable entities in an edge deployment to obtain information about EAS and their available services, based on specified criteria of interest.

EAS discovery enables the EEC to obtain information about available EASs of interest. The discovery of the EASs is based on matching EAS discovery filters provided in the request.

When multiple EASs are discovered for a specific AC, the EEC may select one or more EASs to enable AC communication with one of the selected EASs. The selection algorithm is outside the scope of this specification. Once the EAS is selected, the EEC may subscribe for the ACR event notifications at the EES of the selected EAS, as described in clause 8.8.3.5.2. The EDN configuration information received from ECS may be used for establishing a connection to EAS(s).

EAS discovery may be initiated by the EEC when a certain trigger condition at the UE is met. Some examples are as follows:

- AC related updates available at the EEC (e.g. due to AC installation/re-installation/activation), AC requesting application server access;
- Lifetime received via EAS discovery response specified in clause 8.5.3 is expired; or
- EEC detects the need of application context relocation as in clause 8.8.

NOTE: When the EEC decides to perform EAS discovery is up to EEC implementation.

8.5.2 Procedures

8.5.2.1 General

Following procedures are supported for EAS discovery:

- Request-response procedure;
- Subscribe-notify procedures for EAS discovery and EAS dynamic information subscription, comprising:
 - Subscription procedure;
 - Subscription update procedure; and
 - Unsubscribe procedure;

8.5.2.2 Request-response model

Pre-conditions:

1. The EEC has received information (e.g. URI, IP address) related to the EES;
2. The EEC has received appropriate security credentials authorizing it to communicate with the EES as specified in clause 8.11; and
3. The EES is configured with ECSP's policy for EAS discovery.

NOTE 1: Details of ECSP's policy are out of scope.

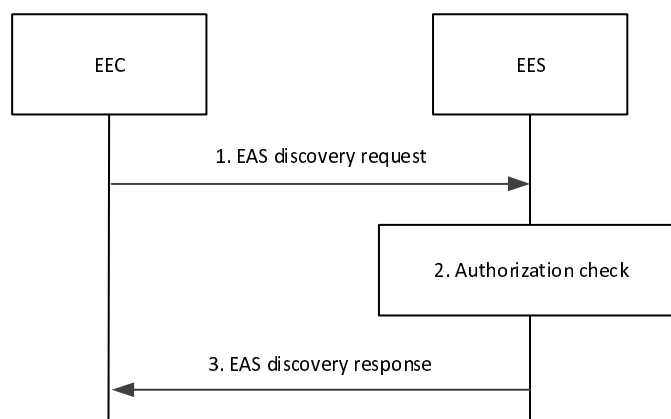


Figure 8.5.2.2-1: EAS Discovery procedure

1. The EEC sends an EAS discovery request to the EES. The EAS discovery request includes the requestor identifier [EECID] along with the security credentials and may include EAS discovery filters and may also include UE location to retrieve information about particular EAS(s) or a category of EASs, e.g. gaming applications, or Edge Applications Server(s) available in certain service areas, e.g. available on a UE's predicted or expected route.
2. Upon receiving the request from the EEC, the EES checks if the EEC is authorized to discover the requested EAS(s). The authorization check may apply to an individual EAS, a category of EASs or to the EDN, i.e. to all the EASs. If UE's location information is not already available, the EES obtains the UE location by utilizing the capabilities of the 3GPP core network as specified in clause 8.10.3. If EAS discovery filters are provided by the EEC, the EES identifies the EAS(s) based on the provided EAS discovery filters and the UE location. If the EEC indicates that service continuity support is required, the EES shall take the indication which ACR scenarios are supported by the AC and the EEC and which of these are preferred by the AC into consideration.

When EAS discovery filters are not provided, then:

- if available, the EES identifies the EAS(s) based on the UE-specific service information at the EES and the UE location;
- EES identifies the EAS(s) by applying the ECSP policy (e.g. based only on the UE location);

NOTE 2: Details of the UE-specific service information and how it is available at the EES is out of scope.

NOTE 3: Both steps are evaluated prior to sending a response.

Upon receiving the request from the EEC, the EES may trigger the EAS management system to instantiate the EAS that matches with EAS discovery filter IEs (e.g. ACID) as in clause 8.12.

3. If the processing of the request was successful, the EES sends an EAS discovery response to the EEC, which includes information about the discovered EASs. For discovered EASs, this includes endpoint information. Depending on the EAS discovery filters received in the EAS discovery request, the response may include additional information regarding matched capabilities, e.g. service permissions levels, KPIs, AC locations(s) that the EASs can support, ACR scenarios supported by the EAS, etc. The EAS discovery response may contain a list of EASs. This list may be based on EAS discovery filters containing a Geographical or Topological Service Area, e.g. a route, included in the EAS discovery request by the EEC.

If the EES is unable to determine the EAS information using the inputs in the EAS discovery request, UE-specific service information at the EES or the ECSP policy, the EES shall reject the EAS discovery request and respond with an appropriate failure cause.

If the EEC is not registered with the EES, and ECSP policy requires the EEC to perform EEC registration prior to EAS discovery, the EES shall include an appropriate failure cause in the EAS discovery response indicating that EEC registration is required.

If the UE location and predicted/expected UE locations, provided in the EAS discovery request, are outside the Geographical or Topological Service Area of an EAS, then the EES shall not include that EAS in the discovery response. The discovery response may include EAS(s) that cannot serve the UE at its current location if a predicted/expected UE location was provided in the EAS discovery request.

Upon receiving the EAS discovery response, the EEC uses the endpoint information for routing of the outgoing application data traffic to EAS(s), as needed, and may provide necessary notifications to the AC(s). The EEC may use the border or overlap between EAS Geographical Service Areas for service continuity purposes. The EEC may cache the EAS information (e.g. EAS endpoint) for subsequent use and avoid the need to repeat step 1. If the Lifetime IE is included in the response, the EEC may cache the EAS information only for the duration specified by the Lifetime IE.

NOTE 4: Within the duration specified by the Lifetime IE, the cached EAS Profile can be updated (e.g. according to notifications from the EES for changes of EAS information due to EAS status change) or the cached EAS Profile can be invalidated due to new EAS information discovery (e.g. due to UE mobility). The EEC can update or invalidate the cached EAS information (e.g. on PDU Session Release or Modification Command).

NOTE 5: The AC can cache the EAS information (e.g. EAS endpoint) for subsequent use. In the case of the cached information needing to be updated or invalidated, the mechanisms for the EEC to notify the AC is up to implementation and is not specified in the current release of the present document.

NOTE 6: The EEC can use the EAS information provided by the discovery procedure to perform service continuity planning, for example when ultra-low latency ACR is required.

If the EAS discovery request fails, the EEC may resend the EAS discovery request, taking into account the received failure cause. If the failure cause indicated that EEC registration is required, the EEC shall perform an EEC registration before resending the EAS discovery request.

8.5.2.3 Subscribe-notify model

8.5.2.3.1 General

Clause 8.5.2.3.2 and clause 8.5.2.3.3 together illustrate the EAS discovery procedure based on Subscribe/Notify model.

Clause 8.5.2.3.4 illustrates the EAS discovery update procedure.

Clause 8.5.2.3.5 illustrates the EAS discovery unsubscribe procedure.

8.5.2.3.2 Subscribe

Figure 8.5.2.3.2-1 illustrates the EAS discovery subscription procedure between the EEC and the EES. This subscription enables EES to inform EEC of various EAS discovery related events of interest to EEC (e.g. EAS discovery notification and EAS dynamic information).

Pre-conditions:

1. The EEC has received information (e.g. URI, IP address) related to the EES;
2. The EEC has received appropriate security credentials authorizing it to communicate with the EES as specified in clause 8.11;
3. The EES is configured with ECSP's policy for EAS discovery; and
4. The EEC has optionally acquired a Notification Target Address to be used in its subscriptions to notifications.

NOTE 1: Details of ECSP's policy are out of scope.

NOTE 2: How the EEC acquires the notification target address or a notification channel URI to receive the notifications is out of scope of this release. The notification target address can terminate at the EEC (e.g. in an IoT device) if the deployment supports EEC reachability, or it can terminate at a push notification service. Details of the push notification service are out of scope of this release.

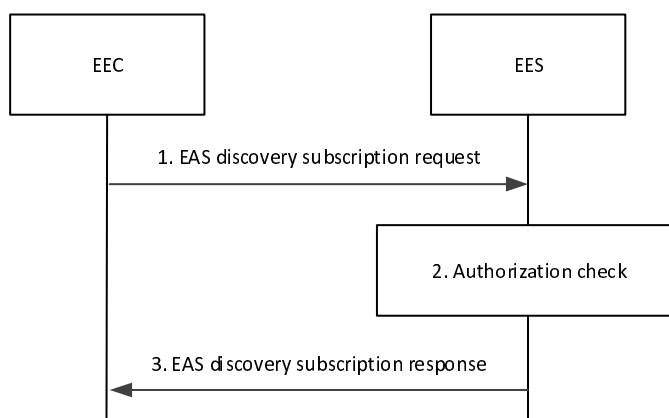


Figure 8.5.2.3.2-1: EAS discovery subscription

1. The EEC sends an EAS discovery subscription request to the EES. The EAS discovery subscription request includes the EECID along with the security credentials, Event ID, and may include EAS discovery filters and EAS dynamic information filters to subscribe to information about particular EAS(s) or a category of EASs (e.g. gaming applications) or dynamic information about EAS(s).
2. Upon receiving the request from the EEC, the EES checks if the EEC is authorized to subscribe for information of the requested EAS(s). The authorization check may apply to an individual EAS, a category of EASs or to the EDN, i.e. to all the EASs. The EES may utilize the capabilities (e.g. UE location) of the 3GPP core network as specified in clause 8.10.3. If the request is authorized, the EES creates and stores the subscription for EAS discovery.
3. If the processing of the request was successful, the EES sends an EAS discovery subscription response to the EEC, which includes the subscription identifier and may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the EEC shall send an EAS discovery subscription update request prior to the expiration time. If an EAS discovery subscription update request is not received prior to the expiration time, the EES shall treat the EEC as implicitly unsubscribed.

If the EES is unable to determine the EAS information using the inputs in the EAS discovery subscription request, UE-specific service information at the EES or the ECSP policy, the EES shall reject the EAS discovery subscription request and respond with an appropriate failure cause.

If the EEC is not registered with the EES, and ECSP policy requires the EEC to perform EEC registration prior to EAS discovery, the EES shall include an appropriate failure cause in the EAS discovery response indicating that EEC registration is required.

If the EAS discovery subscription request fails, the EEC may resend the EAS discovery subscription request again, taking into account the received failure cause. If the failure cause indicated that EEC registration is required, the EEC shall perform an EEC registration before resending the EAS discovery subscription request.

8.5.2.3.3 Notify

Figure 8.5.2.3.3-1 illustrates the EAS discovery notification procedure between the EEC and the EES.

Pre-conditions:

1. The EEC has subscribed with the EES for the EAS discovery information as specified in clause 8.5.2.3.2.

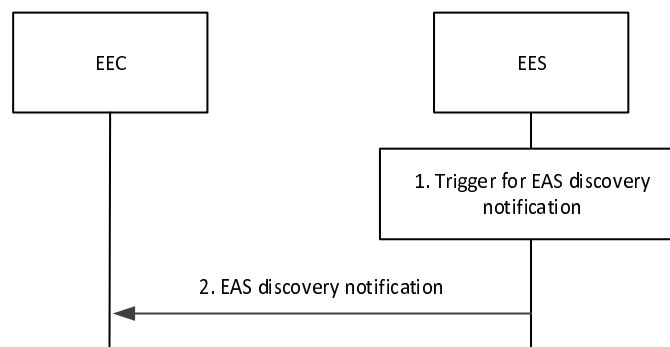


Figure 8.5.2.3.3-1: EAS discovery notification

1. An event occurs at the EES that satisfies trigger conditions for notifying (e.g. to provide EAS discovery information or EAS dynamic information) a subscribed EEC. If UE's location information is not already available, the EES obtains the UE location by utilizing the capabilities of the 3GPP core network as specified in clause 8.10.2. If EAS discovery filters were provided by the EEC during subscription creation, the EES identifies the EAS(s) based on the provided EAS discovery filters and the UE location. If the EEC indicates that service continuity support is required, the EES shall take the indication which ACR scenarios are supported by the AC and the EEC and which of these are preferred by the AC into consideration.

If EAS discovery filters were not provided, then:

- if available, the EES identifies the EAS(s) based on the UE-specific service information at the EES and the UE location;
- EES identifies the EAS(s) by applying the ECSP policy (e.g. based only on the UE location);

NOTE 1: Details of the UE-specific service information and how it is available at the EES is out of scope.

NOTE 2: Both steps are evaluated prior to sending a response.

If the UE is located outside the Geographical or Topological Service Area of an EAS, then the EES shall not include this EAS in the EAS discovery notification.

2. The EES sends an EAS discovery notification to the EEC with the EAS information determined in step 1.

8.5.2.3.4 Subscription update

Figure 8.5.2.3.4-1 illustrates the EAS discovery subscription update procedure between the EEC and the EES.

Pre-conditions:

1. The EEC has subscribed with the EES for the EAS discovery information as specified in clause 8.5.2.3.2

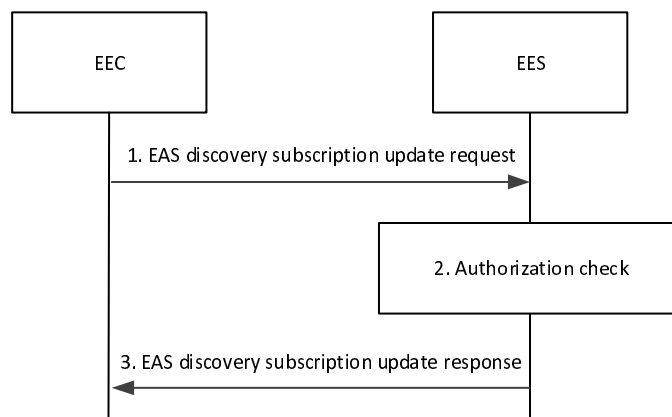


Figure 8.5.2.3.4-1: EAS discovery subscription update

1. The EEC sends an EAS discovery subscription update request to the EES. The EAS discovery subscription update request includes the security credentials and the subscription identifier. It may also include EAS discovery filters, EAS dynamic information filters and/or proposed expiration time for the updated subscription.
2. Upon receiving the request from the EEC, the EES checks if the EEC is authorized to update the subscription information. The EES may utilize the capabilities (e.g. UE location) of the 3GPP core network as specified in clause 8.10.3. If the request is authorized, the EES updated the stored subscription for EAS discovery.
3. The EES sends an EAS discovery subscription update response to the EEC, which may include the expiration time, indicating when the updated subscription will automatically expire. To maintain the subscription, the EEC shall send an EAS discovery subscription update request prior to the expiration time. If an EAS discovery subscription update request is not received prior to the expiration time, the EES shall treat the EEC as implicitly unsubscribed.

8.5.2.3.5 Unsubscribe

Figure 8.5.2.3.5-1 illustrates the EAS discovery unsubscribe procedure between the EEC and the EES.

Pre-conditions:

1. The EEC has subscribed with the EES for notification (e.g. EAS discovery information and EAS dynamic information) as specified in clause 8.5.2.3.2

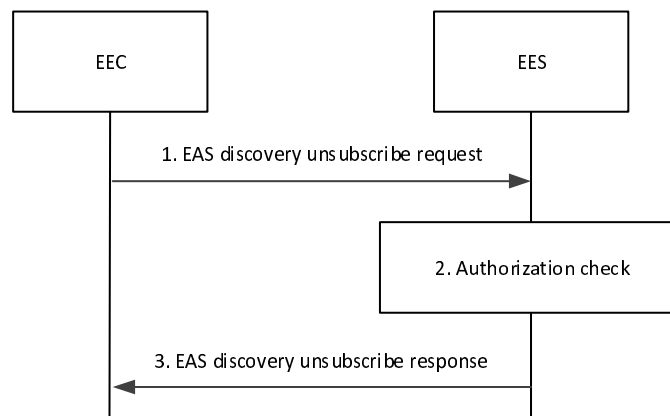


Figure 8.5.2.3.5-1: EAS discovery unsubscribe

1. The EEC sends an EAS discovery unsubscribe request to the EES. The EAS discovery unsubscribe request includes the security credentials of the EEC along with the subscription identifier.
2. Upon receiving the request, the EES performs an authorization check to verify whether the EEC has authorization to perform the operation. If authorized, the EES cancels the subscription for provisioning as requested in step 1.
3. The EES responds with an EAS discovery unsubscribe response.

8.5.3 Information flows

8.5.3.1 General

The following information flows are specified for EAS discovery:

- EAS discovery request and response;
- EAS discovery subscription, notification, subscription update and unsubscribe; and
- EAS dynamic information subscription, notification, subscription update and unsubscribe.

8.5.3.2 EAS discovery request

Table 8.5.3.2-1 describes information elements for the EAS discovery request. Table 8.5.3.2-2 provides further detail about the EAS Discovery Filter information element.

Table 8.5.3.2-1: EAS discovery request

Information element	Status	Description
Requestor identifier	M	The ID of the requestor (e.g. EECID)
UE Identifier	O	The identifier of the UE (i.e. GPSI or identity token)
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EAS discovery filters	O	Set of characteristics to determine required EASs, as detailed in Table 8.5.3.2-2.
UE location	O	The location information of the UE. The UE location is described in clause 7.3.2.
Target DNAI (NOTE)	O	Target DNAI information which can be associated with potential T-EAS(s)
EEC Service Continuity Support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC or, if this message is sent by the EEC to discover a T-EAS, which ACR scenario(s) are intended to be used for the ACR.
EES Service Continuity Support (NOTE)	O	The IE indicates if the S-EES supports service continuity or not. The IE also indicates which ACR scenarios are supported by the S-EES or, if the EAS discovery is used for an S-EES executed ACR according to clause 8.8.2.5, which ACR scenario is to be used for the ACR.
EAS Service Continuity Support (NOTE)	O	The IE indicates if the S-EAS supports service continuity or not. The IE also indicates which ACR scenarios are supported by the S-EAS or, if the EAS discovery is used for an S-EAS decided ACR according to clause 8.8.2.4, which ACR scenario is to be used for the ACR.
NOTE: This IE shall not be included when the request originates from the EEC.		

Table 8.5.3.2-2: EAS discovery filters

Information element	Status	Description
List of AC characteristics (NOTE 1)	O	Describes the ACs for which a matching EAS is needed.
> AC profile (NOTE 2)	M	AC profile containing parameters used to determine matching EAS. AC profiles are further described in Table 8.2.2-1.
List of EAS characteristics (NOTE 1, NOTE 3)	O	Describes the characteristic of required EASs.
> EASID	O	Identifier of the required EAS.
> EAS provider identifier	O	Identifier of the required EAS provider
> EAS type	O	The category or type of required EAS (e.g. V2X)
> EAS schedule	O	Required availability schedule of the EAS (e.g. time windows)
> EAS Geographical Service Area	O	Location(s) (e.g. geographical area, route) where the EAS service should be available.
> EAS Topological Service Area	O	Topological area (e.g. cell ID, TAI) for which the EAS service should be available. See possible formats in Table 8.2.7-1.
> Service continuity support	O	Indicates if the service continuity support is required or not.
> Service permission level	O	Required level of service permissions e.g. trial, gold-class
> Service feature(s)	O	Required service features e.g. single vs. multi-player gaming service
NOTE 1: Either "List of AC characteristics" or "List of EAS characteristics" shall be present.		
NOTE 2: "Preferred ECSP list" IE shall not be present.		
NOTE 3: The "List of EAS characteristics" IE must include at least one optional IE, if used as an EAS discovery filter.		

8.5.3.3 EAS discovery response

Table 8.5.3.3-1 describes information elements for the EAS discovery response from the EES to the EEC.

Table 8.5.3.3-1: EAS discovery response

Information element	Status	Description
Successful response	O	Indicates that the EAS discovery request was successful.
> Discovered EAS list	O	List of discovered EAS(s). Each element includes the information described below.
>> EAS profile	M	Profile of the EAS. Each element is described in clause 8.2.4
>> Lifetime	O	Time interval or duration during which the information elements in the EAS profile is valid and supposed to be cached in the EEC (e.g. time-to-live value for an EAS Endpoint)
Failure response	O	Indicates that the EAS discovery request failed.
> Cause	O	Indicates the cause of EAS discovery request failure.

8.5.3.4 EAS discovery subscription request

Table 8.5.3.4-1 describes the information elements for EAS discovery subscription request from the EEC to the EES.

Table 8.5.3.4-1: EAS discovery subscription request

Information element	Status	Description
EECID	M	Unique identifier of the EEC.
UE Identifier	O	The identifier of the UE (i.e. GPSI or identity token)
Event ID	M	Event ID: - EAS availability change - EAS dynamic information change
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
Notification Target Address	O	The Notification target address (e.g. URL) where the notifications destined for the EEC should be sent to.
EAS discovery filters	O	Set of characteristics to determine matching EASs (as detailed in Table 8.5.3.2-2). Applicable for "EAS availability change" event
EAS dynamic information filters	O	List of dynamic information changes (as detailed in Table 8.5.3.4-2) about EAS, the EEC is interested in. Applicable for "EAS dynamic information change" event
EEC Service Continuity Support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC.
Proposed expiration time	O	Proposed expiration time for the subscription

Table 8.5.3.4-2: EAS dynamic information filters

Information element	Status	Description
List of dynamic information filters	M	List of EAS dynamic information required by the EEC per EAS.
> EASID	M	Identifier of the EAS
> ACIDs	O	Flag to notify change in list of ACIDs served by the EAS
> EAS Description	O	Flag to notify change in description of the EAS.
> EAS Endpoint	O	Flag to notify change in EAS endpoint
> EAS Features	O	Flag to notify any change in features provided by the EAS
> EAS Schedule	O	Flag to notify change in availability schedule of the EAS (e.g. time windows)
> EAS Service Area	O	Flag to notify change in change in geographical service area that the EAS serves
> EAS Service KPIs	O	Flag to notify change in characteristics of the EAS.
> EAS Status	O	Flag to notify change in the status of the EAS (e.g. enabled, disabled, etc.)
> Service continuity support	O	Flag to notify change in EAS support for service continuity.

8.5.3.5 EAS discovery subscription response

Table 8.5.3.5-1 describes the information elements for EAS discovery subscription response from the EES to the EEC.

Table 8.5.3.5-1: EAS discovery subscription response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.5.3.6 EAS discovery notification

Table 8.5.3.6-1 describes the information elements for EAS discovery notification from the EES to the EEC.

Table 8.5.3.6-1: EAS discovery notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the EES for the request
Event ID	M	Either EAS discovery notification or EAS dynamic information notification
EAS list	O	List of EAS profiles. Each element includes the information described below.
> EAS profile	M	Profile of the EAS. Each element is described in clause 8.2.4
> Lifetime	O	Time interval or duration during which the information elements in the EAS profile is valid and supposed to be cached in the EEC (e.g. time-to-live value for an EAS Endpoint)

8.5.3.7 EAS discovery subscription update request

Table 8.5.3.7-1 describes the information elements for EAS discovery subscription update request from the EEC to the EES.

Table 8.5.3.7-1: EAS discovery subscription update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be updated
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
Proposed expiration time	O	Proposed expiration time for the subscription
EAS discovery filters	O	Set of characteristics to determine required EASs, as detailed in Table 8.5.3.2-2.
EAS dynamic information filters	O	List of dynamic information about EAS, the EEC is interested in, as detailed in Table 8.5.3.4-2.
EEC Service Continuity Support	O	Indicates if the EEC supports service continuity or not. The IE also indicates which ACR scenarios are supported by the EEC.

8.5.3.8 EAS discovery subscription update response

Table 8.5.3.8-1 describes the information elements for EAS discovery subscription update response from the EES to the EEC.

Table 8.5.3.8-1: EAS discovery subscription update response

Information element	Status	Description
Successful response	O	Indicates that the subscription update request was successful.
> Expiration time	O	Indicates the expiration time of the updated subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription update request failed.
> Cause	O	Indicates the cause of subscription update request failure

8.5.3.9 EAS discovery unsubscribe request

Table 8.5.3.9-1 describes the information elements for EAS discovery unsubscribe request from the EEC to the EES.

Table 8.5.3.9-1: EAS discovery unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be unsubscribed
Security credentials	M	Security credentials of the EEC

8.5.3.10 EAS discovery unsubscribe response

Table 8.5.3.10-1 describes the information elements for EAS discovery unsubscribe response from the EES to the EEC.

Table 8.5.3.10-1: EAS discovery unsubscribe response

Information element	Status	Description
Successful response	O	Indicates that the unsubscribe request was successful.
Failure response	O	Indicates that the unsubscribe request failed.
> Cause	O	Indicates the cause of unsubscribe request failure

8.5.4 APIs

8.5.4.1 General

Table 8.5.4.1-1 illustrates the API for EAS discovery.

Table 8.5.4.1-1: Eees_EASDiscovery API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_EASDiscovery	Request	Request/Response	EEC
	Subscribe	Subscribe/Notify	EEC
	Notify		
	UpdateSubscription		
	Unsubscribe		

8.5.4.2 Eees_EASDiscovery_Request operation

API operation name: Eees_EASDiscovery_Request

Description: The consumer requests for one time EAS discovery information.

Inputs: See clause 8.5.3.2.

Outputs: See clause 8.5.3.3.

See clause 8.5.2.2 for details of usage of this operation.

8.5.4.3 Eees_EASDiscovery_Subscribe operation

API operation name: Eees_EASDiscovery_Subscribe

Description: The consumer subscribes for EAS discovery information.

Inputs: See clause 8.5.3.4.

Outputs: See clause 8.5.3.5.

See clause 8.5.2.3.2 for details of usage of this operation.

8.5.4.4 Eees_EASDiscovery_Notify operation

API operation name: Eees_EASDiscovery_Notify

Description: The consumer is notified with EAS discovery and/or EAS dynamic information.

Inputs: See clause 8.5.3.6.

Outputs: None.

See clause 8.5.2.3.3 for details of usage of this operation.

8.5.4.5 Eees_EASDiscovery_UpdateSubscription operation

API operation name: Eees_EASDiscovery_UpdateSubscription

Description: The consumer updates an existing subscription for EAS discovery information.

Inputs: See clause 8.5.3.7.

Outputs: See clause 8.5.3.8.

See clause 8.5.2.3.4 for details of usage of this operation.

8.5.4.6 Eees_EASDiscovery_Unsubscribe operation

API operation name: Eees_EASDiscovery_Unsubscribe

Description: The consumer cancels an existing subscription for EAS discovery information.

Inputs: See clause 8.5.3.9.

Outputs: See clause 8.5.3.10.

See clause 8.5.2.3.5 for details of usage of this operation.

8.6 EES capability exposure to EAS

8.6.1 General

This clause describes service capability APIs exposed by the EES to the EAS(s). The service capability APIs exposed include EES capabilities and exposed 3GPP Core Network capabilities. The 3GPP Core Network capabilities may be exposed from EES to the EAS(s).

The 3GPP Core Network capabilities APIs which are enhanced for exposure are also specified in this clause.

NOTE: When the ACR occurs, the new EAS can re-subscribe the EES capability exposure services on the T-EES.

8.6.2 UE location API

8.6.2.1 General

The EES exposes the UE location API to the EAS in order to support tracking or checking the valid location of the UE. The UE location API exposed by the EES relies on the 3GPP core network capabilities as specified in clause 8.10.3.

The EAS can request UE location API for one-time reporting to check current UE location and for continuous reporting to track UE's location.

The UE location API supports both request-response for one-time queries (in order to check UE's current location) as well as subscribe-notify models for providing UE's location to EAS on a continuous basis and enabling the EAS to track UE's location (as UE location changes).

8.6.2.2 Procedures

8.6.2.2.1 General

8.6.2.2.2 Request-response model

Figure 8.6.2.2.2-1 illustrates the interactions between the EES and the EAS for one-time location report.

Pre-conditions:

1. The EAS is authorized to discover and to use UE location API provided by the EES.
2. The EES is authorized to use Nnef Event Exposure API for UE location, based on service level agreement with MNO.
3. UE Identifier between EAS and the EES is authorized for the UE location API.

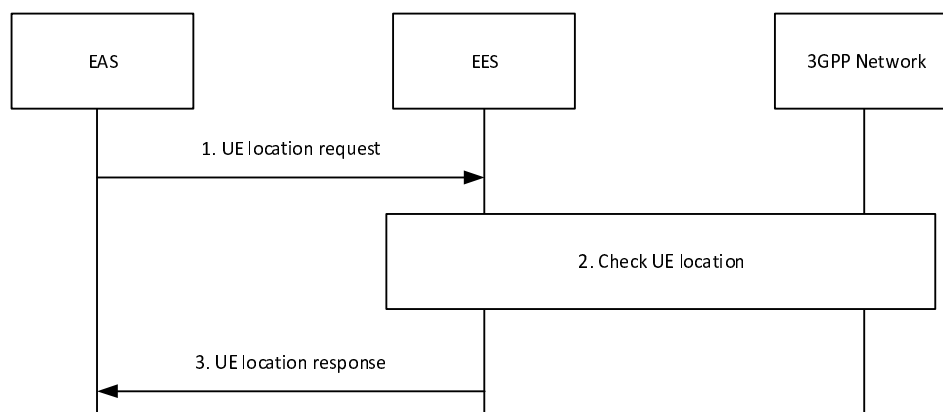


Figure 8.6.2.2-1: UE location API request-response model

1. The EAS sends UE location request to the EES. The UE location request shall include the UE Identifier. It may also include location granularity to indicate requested format of the location e.g. GPS Coordinates, Cell ID, Tracking Area ID, or civic addresses (e.g. streets, districts, etc.), which can be understood by the EAS and location QoS.

NOTE 1: The trigger condition of the UE location API is up to application service logic, which is out of scope of this specification.

2. The EES checks the UE location:
 - a. If the UE location request from the EAS includes the location granularity, the EES considers the location granularity parameter for checking the location of the UE.
 - b. If the EES has a valid locally cached location of the UE, the EES may use this cached UE location to respond to the EAS. Otherwise, the EES utilizes the capabilities of the 3GPP core network as specified in clause 8.10.3.
 - c. The EES may modify the format of the UE location to fit to the location granularity requested from the EAS in the step 1, if supported. For example, if the EES receives the UE location in a format of tracking area ID or cell ID, the EES can modify the representation of the location information to the GPS Coordinates, or civic addresses (e.g. streets, districts, etc.) as requested by the EAS.

NOTE 2: Format modification mechanism of the UE location to fit the location granularity is outside the scope of this specification. Step 2.c. can be performed if the EES is deployed by the PLMN operator.

3. If successful, the EES responds to the EAS with the location of the UE, and optionally the timestamp of the location.

8.6.2.2.3 Subscribe-notify model

8.6.2.2.3.1 General

8.6.2.2.3.2 Subscribe

Figure 8.6.2.2.3.2-1 illustrates the subscribe operation between the EAS and the EES for continuous UE location reporting.

Pre-conditions:

1. The EAS is authorized to discover and to use UE location API provided by the EES;
2. The EES is authorized to use 3GPP network exposure capability (e.g. Nnef Event Exposure API) for UE location, based on service level agreement with MNO; and
3. UE Identifier between EAS and the EES is authorized for the UE location API.

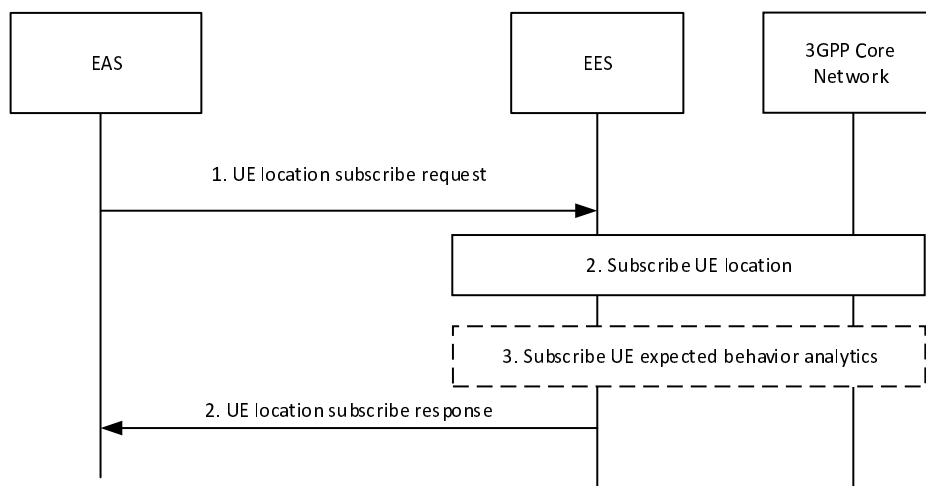


Figure 8.6.2.2.3.2-1: UE location API: Subscribe operation

1. The EAS sends UE location subscribe request to the EES for tracking a UE's location continuously. The UE location subscribe request shall include the UE Identifier or UE group Identifier and may include proposed expiration time. It may also include location granularity to indicate requested format of the location e.g. GPS Coordinates, Cell ID, Tracking Area ID, or civic addresses (e.g. streets, districts, etc.), which can be understood by the EAS and location QoS.
2. The EES checks if the request from the EAS is authorized. If authorized, the EES sends success response to the EAS and utilizes the UE location exposure capability of the 3GPP core network as specified in clause 8.10.3. The EES requests continuous location reporting from the 3GPP system to have up to date location information of the UE.
3. The EES may subscribe to UE expected behaviour analytics (UE mobility) as described in 3GPP TS 23.288 [18].
4. The response includes the subscription identifier and may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the EAS shall send a UE location subscription update request prior to the expiration time. If a UE location subscription update request is not received prior to the expiration time, the EES shall treat the EAS as implicitly unsubscribed. If it is not authorized, the EES sends failure response with rejection cause.

8.6.2.2.3.3 Notify

Figure 8.6.2.2.3.3-1 illustrates the notify operation between the EES and the EAS for continuous location.

Pre-conditions:

1. The EAS has subscribed to UE location API provided by the EES.

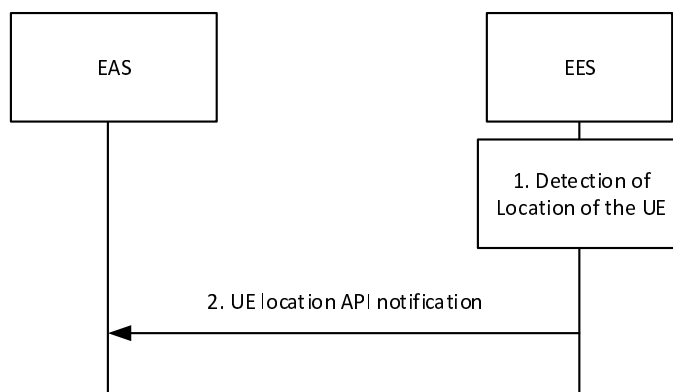


Figure 8.6.2.2.3.3-1: UE location API: Notify operation

1. The EES detects the location of the UE e.g., receiving location of the UE from the 3GPP system. The EES may cache the detected location information locally with timestamp as the latest location information of the UE(s) and start the notification aggregation for a group of UEs. The EES decides whether to aggregate and the aggregation period based on the analytics result received from the 3GPP Core Network, local policy and UE location subscription information received from the EAS. The EES determines to notify the location information of the UE to the EAS which has subscribed for UE's location.
2. The EES sends UE location notification to the EAS. The EES includes the location of the UE(s). Each UE location includes UE ID and location type and may include the location accuracy and the timestamp of the location.

The EES may modify the format of location information to fit to the location granularity requested from the EAS during the subscribe operation, if supported. For example, if the EES receives the UE location in a format of tracking area ID or cell ID, the EES can modify the representation of the location information to the GPS Coordinates, or civic addresses (e.g. streets, districts, etc.) as requested from the EAS.

8.6.2.2.3.4 Subscription update

Figure 8.6.2.2.3.4-1 illustrates the subscription update operation between the EAS and the EES.

Pre-conditions:

1. The EAS has subscribed to UE location API provided by the EES.

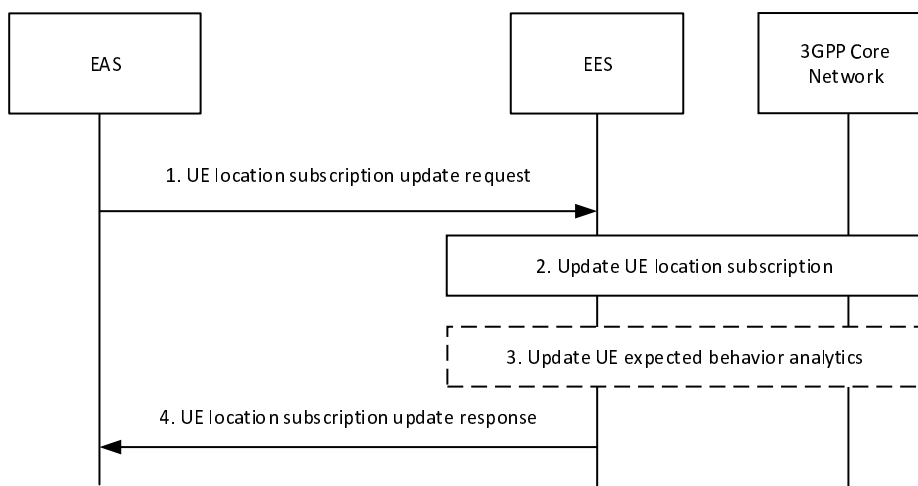


Figure 8.6.2.2.3.4-1: UE location API: Subscription update operation

1. The EAS sends UE location subscription update request to the EES. The request includes the subscription identifier of the subscription to be. The UE location subscription update request may also include proposed expiration time for the updated subscription, updated Location granularity and Location QoS.
2. The EES checks if the request from the EAS is authorized. If authorized, the EES updates the subscription request and may update the UE location subscription in the 3GPP Core Network.
3. The EES may update the subscription to the UE expected behaviour analytics.
4. The EES sends the UE location subscription update response to the EAS.

8.6.2.2.3.5 Unsubscribe

Figure 8.6.2.2.3.5-1 illustrates the unsubscribe operation between the EAS and the EES to stop the UE location notifications.

Pre-conditions:

1. The EAS has subscribed to UE location API provided by the EES.

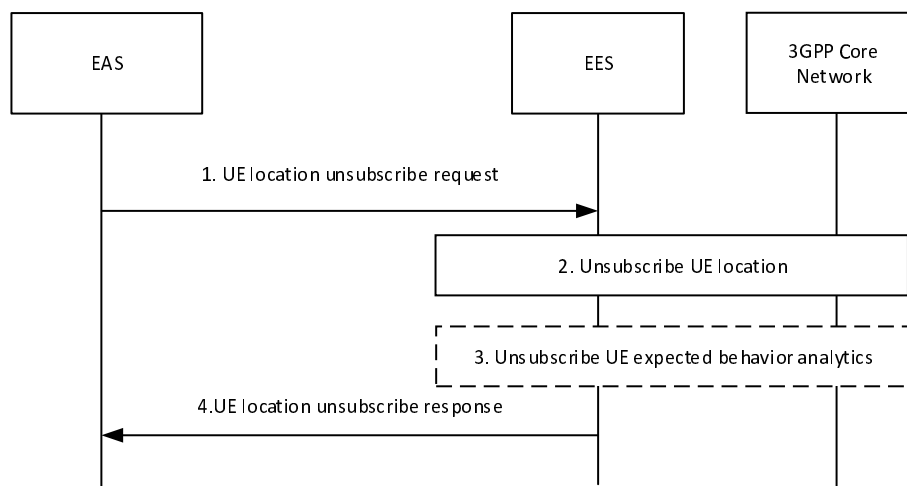


Figure 8.6.2.2.3.5-1: UE location API: unsubscribe operation

1. The EAS sends the UE location unsubscribe request to the EES.
2. The EES checks if the EAS is authorized or not. If authorized, the EES terminates the subscription of the EAS and unsubscribes the UE location from the 3GPP Core Network.
3. The EES unsubscribes from the UE expected behaviour analytics, if applicable.
4. The EES responds to the EAS.

8.6.2.3 Information flows

8.6.2.3.1 General

The following information flows are specified for UE location API:

- UE location request and response; and
- UE location subscription, notification, subscription update and unsubscribe.

8.6.2.3.2 UE location request

Table 8.6.2.3.2-1: UE location request

Information element	Status	Description
UE ID	M	Identifies the UE for which location will be reported (e.g. GPSI)
Security credentials	M	Security credentials of the EAS
Location granularity	O	indicates format of location e.g. GPS Coordinates, Cell ID, Tracking Area ID, or civic addresses (e.g. streets, districts, etc.) that can be understood by the EAS
Location QoS	O	Indicate the location quality of service as described in clause 4.1b of 3GPP TS 23.273 [9].

8.6.2.3.3 UE location response

Table 8.6.2.3.3-1: UE location response

Information element	Status	Description
Successful response	O	Indicates that the UE location request was successful
> UE location	M	Location of the UE
> Timestamp	O	Indicates the age of the UE's location information
> Location accuracy	O	Indicates accuracy of the location information
Failure response	O	Indicates that the subscription request failed
> Cause	O	Indicates the cause of request failure

8.6.2.3.4 UE location subscribe request

Table 8.6.2.3.4-1: UE location subscribe request

Information element	Status	Description
EASID	M	The identifier of the EAS
UE ID (NOTE)	O	Identifies the UE for which location will be reported (i.e GPSI)
UE Group ID (NOTE)	O	Identifies a group of UEs (i.e. internal group ID or external group ID)
Security credentials	M	Security credentials of the EAS
Notification Target Address	M	Notification Target Address of the EAS where the notification is to be sent by the EES
Event reporting information	O	Event Reporting Information as specified in Table 4.15.1-1 of 3GPP TS 23.502 [3], e.g. event reporting mode.
Proposed expiration time	O	Proposed expiration time for the subscription
Location Granularity	O	indicates format of location e.g. GPS Coordinates, Cell ID, Tracking Area ID, or civic addresses (e.g. streets, districts, etc.) that can be understood by the EAS
Location QoS	O	Indicate the location quality of service as described in clause 4.1b of 3GPP TS 23.273 [9].
NOTE: Either UE ID or UE Group ID shall be provided.		

8.6.2.3.5 UE location subscribe response

Table 8.6.2.3.5-1: UE location subscribe response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.6.2.3.6 UE location notification

Table 8.6.2.3.6-1: UE location notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the EES for the request
List of event notifications	M	A list of event notifications for one or more UEs.
> UE ID	M	The identifier of each UE (i.e. GPSI or identity token)
> UE location	M	Location of the UE
> Timestamp	O	Indicates the age of the location information
> Location accuracy	O	Indicates accuracy of the location information
> Location type	M	Indicates whether it is a predictive or actual UE location change.

8.6.2.3.7 UE location subscription update request

Table 8.6.2.3.7-1: UE location subscription update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be updated
Security credentials	M	Security credentials of the EAS
Event reporting information (NOTE)	O	Event Reporting Information as specified in Table 4.15.1-1 of 3GPP TS 23.502 [3], e.g. event reporting mode.
Proposed expiration time (NOTE)	O	Proposed expiration time for the subscription
Notification Target Address (NOTE)	O	Notification Target Address of the EAS where the notification is to be sent by the EES
Location Granularity (NOTE)	O	indicates format of location e.g. GPS Coordinates, Cell ID, Tracking Area ID, or civic addresses (e.g. streets, districts, etc.) that can be understood by the EAS
Location QoS (NOTE)	O	Indicate the location quality of service as described in clause 4.1b of 3GPP TS 23.273 [9].
NOTE: At least one of these IEs is present.		

8.6.2.3.8 UE location subscription update response

Table 8.6.2.3.8-1: UE location subscription update response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.6.2.3.9 UE location unsubscribe request

Table 8.6.2.3.9-1: UE location unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the EES for the request
Security credentials	M	Security credentials of the EAS

8.6.2.3.10 UE location unsubscribe response

Table 8.6.2.3.10-1: UE location unsubscribe response

Information element	Status	Description
Successful response	O	Indicates that the unsubscribe request was successful.
Failure response	O	Indicates that the unsubscribe request failed.
> Cause	O	Indicates the cause of unsubscribe request failure

8.6.2.4 APIs

8.6.2.4.1 General

Table 8.6.2.4.1-1 illustrates the API for UE location.

Table 8.6.2.4.1-1: Eees_UELocation API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_UELocation	Get	Request/Response	EAS
	Subscribe	Subscribe/Notify	EAS
	Notify		
	UpdateSubscription		
	Unsubscribe		

8.6.2.4.2 Eees_UELocation_Get operation

API operation name: Eees_UELocation_Get

Description: The consumer requests one time report of a UE's location.

Inputs: See clause 8.6.2.3.2.

Outputs: See clause 8.6.2.3.3.

See clause 8.6.2.2.2 for details of usage of this operation.

8.6.2.4.3 Eees_UELocation_Subscribe operation

API operation name: Eees_UELocation_Subscribe

Description: The consumer subscribes for continuous reporting of a UE's location.

Inputs: See clause 8.6.2.3.4.

Outputs: See clause 8.6.2.3.5.

See clause 8.6.2.2.3.2 for details of usage of this operation.

8.6.2.4.4 Eees_UELocation_Notify operation

API operation name: Eees_UELocation_Notify

Description: The consumer is notified with report of the UE's location.

Inputs: See clause 8.6.2.3.6.

Outputs: None.

See clause 8.6.2.2.3.3 for details of usage of this operation.

8.6.2.4.5 Eees_UELocation_UpdateSubscription operation

API operation name: Eees_UELocation_UpdateSubscription

Description: The consumer updates an existing subscription for continuous reporting of a UE's location.

Inputs: See clause 8.6.2.3.7.

Outputs: See clause 8.6.2.3.8.

See clause 8.6.2.2.3.4 for details of usage of this operation.

8.6.2.4.6 Eees_UELocation_Unsubscribe operation

API operation name: Eees_UELocation_Unsubscribe

Description: The consumer cancels an existing subscription for continuous reporting of a UE's location.

Inputs: See clause 8.6.2.3.9.

Outputs: See clause 8.6.2.3.10.

See clause 8.6.2.2.3.5 for details of usage of this operation.

8.6.3 ACR management events

8.6.3.1 General

The EES exposes ACR management event notifications of one or more UEs to an EAS. EES also uses ACR management event notifications to inform the EAS of the need to start an ACT or cancel a previously started ACT. ACR management event notifications exposed by the EES may rely on the NEF northbound API for monitoring event of user plane path management event.

This capability exposed by the EES supports:

- "User plane path change". This event supports to detect user plane path change for the application traffic and report the corresponding notification with user plane path change to the EAS.
- "ACR monitoring". This event supports to detect user plane path change for the application traffic, discover the T-EAS(s), and report the corresponding notification with the discovered T-EAS(s).
- "ACR facilitation". This event supports to detect user plane path change for the application traffic, make the decision for ACR, discover the T-EAS(s), influence the traffic for the selected T-EAS and report the corresponding notification with the selected T-EAS.
- "ACT start/stop". This event informs the EAS the need to start or stop an ACT towards or from another EAS for a particular UE.

The availability of the ACR management event notifications relying on the user plane path management event notification service exposed by 5GC may change due to UE mobility between 5GC and EPC. If an EES exposes ACR event notifications to EAS(s) for a UE by relying on the 3GPP Core Network northbound API for user plane path management notifications, the EES monitors the availability of the northbound API for UE(s) served by the EAS (e.g. by utilizing Nnef_APISupportCapability as described in 3GPP TS 23.502 [3]) and provides the availability information to the EAS accordingly. If CAPIF is supported, the EES determines if the ACR management event API is available and able to be exposed to the EAS for a UE via the Availability of service APIs event notifications provided by the CAPIF core function as defined in 3GPP TS 23.222 [6].

8.6.3.2 Procedures

8.6.3.2.1 General

8.6.3.2.2 Subscribe

Figure 8.6.3.2.2-1 illustrates the subscribe operation between the EAS and the EES for ACR management event notifications.

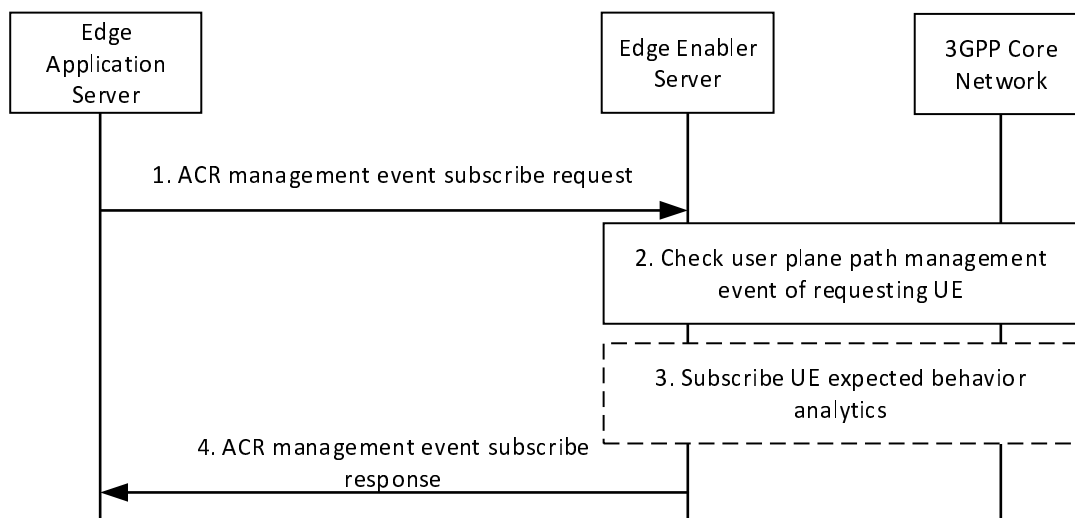


Figure 8.6.3.2.2-1: ACR management event API: Subscribe operation

1. The EAS sends ACR management event subscribe request (e.g. tracking the UE's user plane path change continuously). The EAS shall include UE Identifier or UE group Identifier for "user plane path change", "ACR monitoring" and "ACR facilitation" events.
 - a. The EAS may include the "user plane path change" event to indicate the EES to notify the EAS when the EES detects there is a user plane path change for the application traffic and the EAS may include Subscription Type (Early and/or Late notification defined in clause 5.6.7 of 3GPP TS 23.501 [2]) and/or Indication of EAS Acknowledgement in the event subscription.
 - b. The EAS may include the "ACR monitoring" event to indicate the EES to notify the EAS when the EES detects there is a need for the ACR (e.g. when T-EAS is available at the target DNAI). The EAS may also include the Event Filters to specify the conditions to match for notifying the event, e.g., inter-EDN mobility, intra-EDN mobility.
 - c. The EAS may include the "ACR facilitation" event to request the EES to make the decision for ACR, discover the T-EAS(s), influence the traffic for the selected T-EAS and notify the S-EAS of the selected T-EAS.
 - d. The EAS may include the "ACT start/stop" event to indicate the EES to notify the EAS of the need for start or stop ACT to or from another EAS for a particular UE.
2. The EES checks if the EAS is authorized for this operation.

If authorized, and if the subscription in step 1 includes at least one of the "user plane path change", "ACR monitoring" and "ACR facilitation" events, the EES checks if there exists a subscription with the 3GPP core network for the user plane path management event notifications corresponding to the UE information obtained in step 1 as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3], which may be triggered by other EAS for the same UE. The EES checks the availability of the user plane path management event service for the UE.

- a. if a subscription with 3GPP core network does not exist, then the EES subscribes with the 3GPP core network (PCF, NEF or SCEF+NEF) for the user plane path management event notifications of the UE as

described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3] If the EAS provides Subscription Type and/or Indication of EAS Acknowledgement, the EES include the type of subscription and/or the indication of "AF acknowledgement to be expected" as information on AF subscription to corresponding SMF events within the AF Request;

- b. if a subscription with 3GPP core network exists, then the EES uses the locally cached user plane path management event notification information of the UE to respond to the EAS.

The EES stores the subscription related to the EAS.

3. If the event is "user plane path change", the EES may subscribe to UE expected behaviour analytics (UE mobility and UE communication) for the group of UEs as described in 3GPP TS 23.288 [18].
4. If EAS is authorized, the EES responds with ACR management event subscribe response. If EAS is not authorized, the EES provides a rejection response with cause information.

If the target UE and the 3GPP network support mobility between 5GC and EPC, the EES monitors the availability of the user plane path management event notification from the 3GPP network by utilizing Nnef_APISupportCapability or Availability of service APIs event notifications provided by the CAPIF core function.

8.6.3.2.3 Notify

Figure 8.6.3.2.3-1 illustrates the notify operation between the EES and the EAS for continuous ACR management event notifications.

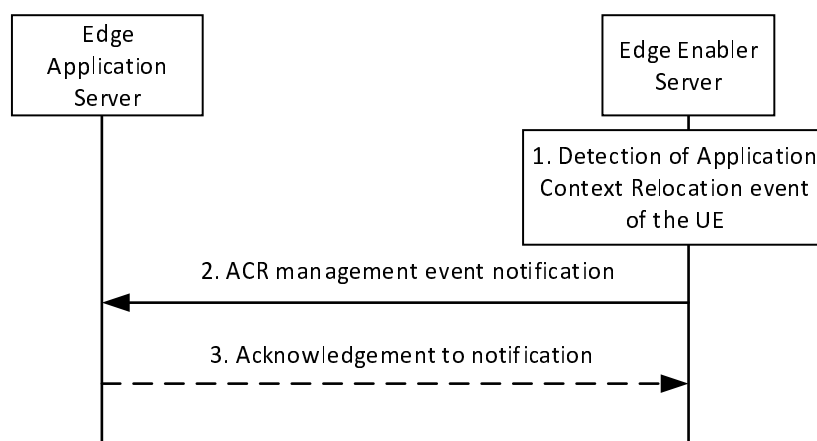


Figure 8.6.3.2.3-1: ACR management event API: Notify operation

1. The EES detects the ACR management event of the UE (e.g. receiving User plane path management event notification for the UE from the 3GPP core network).
 - a. If "user plane path change" Event is subscribed, the EES may cache the detected User plane path management event notification locally with timestamp as the latest information of the UE(s) and start the notification aggregation for a group of UEs. The EES decides whether to aggregate and the aggregation period based on the analytics result received from the 3GPP Core Network, local policy and User Plane path management subscription information received from the EAS. The EES determines to notify the user plane path management event notification information (e.g., DNAI) to the EASs which has subscribed for the "user plane path management" event.
 - b. If "ACR monitoring" Event is subscribed, based on the detected user plane path change report sent from the 3GPP core network, the EES checks whether the target DNAI is in the EAS profile of the subscribing EAS, if not it further checks whether a T-EAS is available at the target DNAI as described in steps 2-4 of clause 8.8.3.2. If a T-EAS is available, the EES notifies the EAS with T-EAS endpoint; otherwise this event notification will not be sent. Also, when the EES receives the ACR request from the EEC, the EES decides to send the notification to the EAS.

- c. If "ACR facilitation" Event is subscribed, based on the detected user plane path change report sent from the 3GPP core network, the EES checks whether the target DNAI is in the EAS profile of the subscribing EAS, if not it further checks whether a T-EAS is available at the target DNAI as described in steps 2-4 of clause 8.8.3.2. If a T-EAS is available, the EES selects the T-EAS from the discovered EAS list and applies the AF traffic influence with the N6 routing information of the selected T-EAS in the 3GPP Core Network. The EES also notifies the S-EAS with the selected T-EAS endpoint.
 - d. If "ACT start/stop" event is subscribed, during the ACR launch if the EEC indicates the need to notify the EAS in the ACR request as described in clause 8.8.3.4, the EES shall send notification to the EAS to inform it about the need to start or stop the ACT to or from another EAS.
2. The EES sends ACR management event notification to the EAS. The EES includes the ACR management event notification information of the UE(s) and optionally the timestamp. If the event triggering the notification is DNAI change, the timestamp can be included to indicate the age of the user plane path management event notification information. The EES may only provide part of information included in the user plane path management event notification from 3GPP network (e.g. target DNAI). If the EAS had provided "Indication of EAS acknowledgement", the EES waits for acknowledgement from the EAS before it sends AF acknowledgement to the 3GPP core network.
- If the event is "ACT start/stop", the notification shall include the endpoint address of the other EAS and the UE ID.
3. If the EAS had included Indication of EAS Acknowledgement within ACR path management event subscribe request described in clause 8.6.3.2.1, the EAS sends EAS Acknowledgement as a response to ACR management event notification to the EES either immediately or after the required ACT is completed. The EAS may reply in negative, e.g., the EAS may determine not to perform ACR. Then, the EES sends the AF acknowledgement to the 3GPP core network.

8.6.3.2.4 Subscription update

Figure 8.6.3.2.4-1 illustrates the subscription update operation between the EAS and the EES for ACR management event notifications.

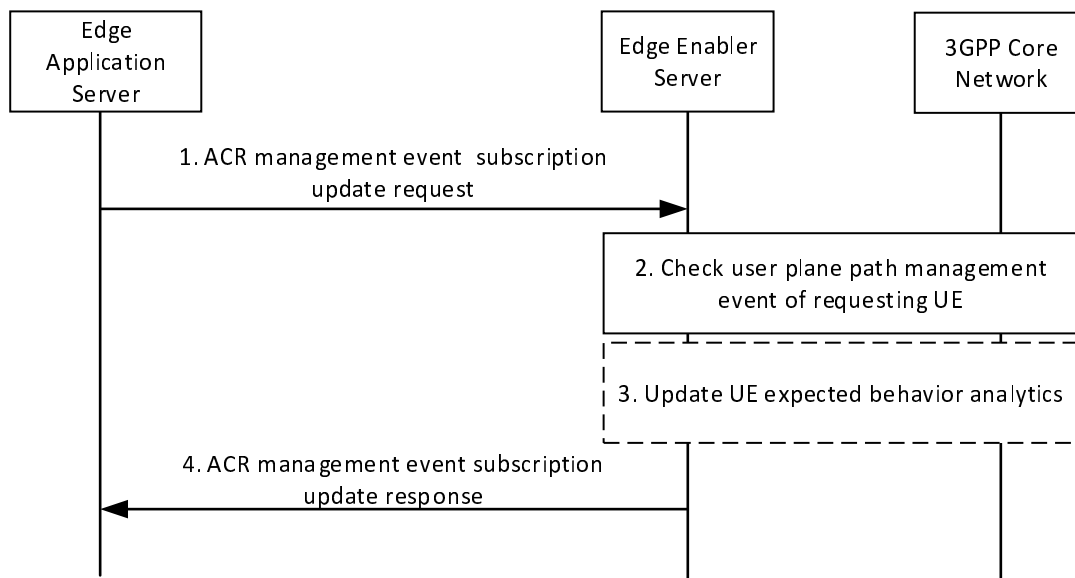


Figure 8.6.3.2.4-1: ACR management event API: Subscription update operation

1. The EAS sends ACR management event subscription update request to update an existing subscription. The subscription update request may include Event ID, Event Filter, Event Report, Subscription Type (Early and/or Late notification defined in clause 5.6.7 of 3GPP TS 23.501 [2]) and/or Indication of EAS Acknowledgement.
2. The EES checks if the EAS is authorized for the operation.

If authorized and if the subscription in step 1 includes only "ACT start/stop" event, the EES stores the updated subscription related to the EAS and step 3 is skipped.

If authorized, and if the subscription in step 1 includes at least one of the "user plane path change", "ACR monitoring" and "ACR facilitation" events, the EES checks if there exists a subscription with the 3GPP core network for the user plane path management event notifications corresponding to the updated information obtained in step 1 as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3], which may be triggered by other EAS for the same UE.

- a. if a subscription with 3GPP core network does not exist corresponding to the updated information, then the EES subscribes with the 3GPP core network (PCF, NEF or SCEF+NEF) for the user plane path management event notifications of the UE as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3] If the EAS provides Subscription Type and/or Indication of EAS Acknowledgement, the EES includes the type of subscription and/or the indication of "AF acknowledgement to be expected" as information on AF subscription to corresponding SMF events within the AF Request;
- b. if a subscription with 3GPP core network exists corresponding to the updated information, then the EES uses the locally cached user plane path management event notification information of the UE to respond to the EAS.

The EES stores the updated subscription related to the EAS.

3. The EES may update the subscription to the UE expected behaviour analytics.
4. The EES responds with ACR management event subscription response.

8.6.3.2.5 Unsubscribe

Figure 8.6.3.2.5-1 illustrates the unsubscribe operation between the EAS and the EES for ACR management event notifications.

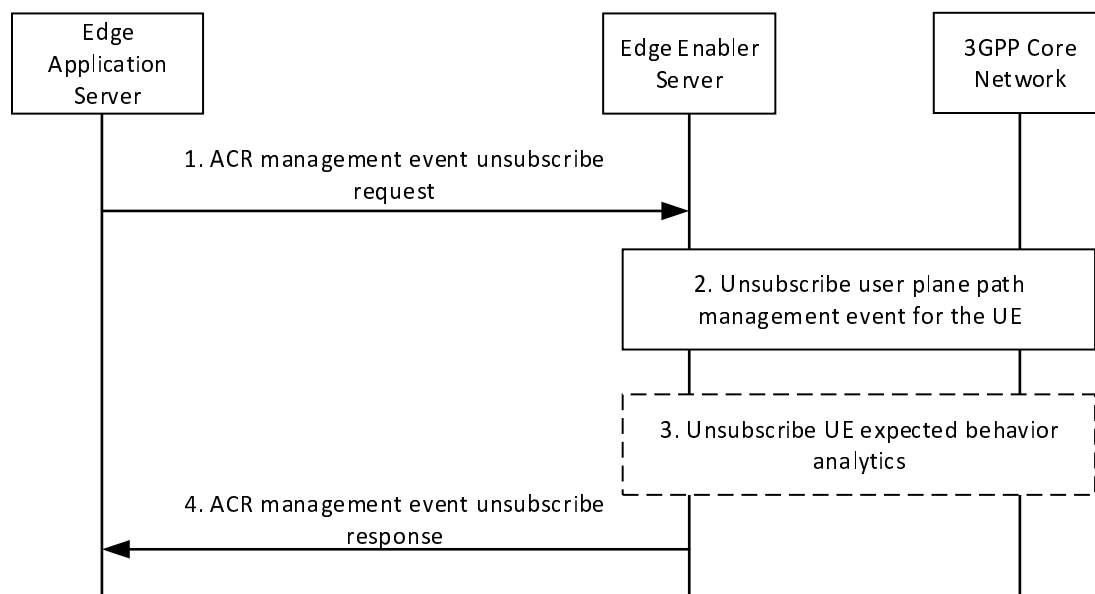


Figure 8.6.3.2.5-1: ACR management event API: Unsubscribe operation

1. The EAS sends ACR management event unsubscribe request to the EES to cancel the ACR management event subscription.
2. The EES checks if another EAS requires to track the UE's user plane path change or not. If not, the EES unsubscribes the user plane path management event notifications from the 3GPP core network for the corresponding UE.

3. The EES unsubscribes from the UE expected behaviour analytics, if applicable.
4. The EES checks if the EAS is authorized for the operation. If authorized, the EES removes the subscription related to the EAS and sends ACR management event unsubscribe response to the EAS.

8.6.3.3 Information flows

8.6.3.3.1 General

The following information flows are specified for ACR management event API:

- ACR management event subscription, notification, subscription update and unsubscribe.

8.6.3.3.2 ACR management event subscribe request

Table 8.6.3.3.2-1 describes the information elements for an ACR management event subscribe request from the EAS to the EES.

Table 8.6.3.3.2-1: ACR management event subscribe request

Information element	Status	Description
EASID	M	The identifier of the EAS
Security credentials	M	Security credentials of the EAS
UE ID (NOTE 1)	O	The identifier of the UE (i.e. GPSI or identity token)
UE Group ID (NOTE 1)	O	Identifies a group of UEs (i.e. internal group ID or external group ID)
Event ID(s)	M	Event ID: - user plane path change - ACR monitoring - ACR facilitation - ACT start/stop
Event Report (NOTE 2)	O	Event Reporting Information as specified in 3GPP TS 23.502 [3]
Notification Target Address	M	Notification Target Address of the EAS where the notification is to be sent by the EES
Type of subscription	O	Indicates Early and/or Late notification to inform if the notification needs to be received before and/or after UP path configuration. Applicable for the "user plane path change" event.
Indication of EAS acknowledgement	O	This IE indicates the EES to include indication of "AF acknowledgement to be expected" within the AF request for subscribing UP path management events to 3GPP network and that the EAS will provide an acknowledgement as a response for the notifications of UP path management events to the EES. Applicable for the "user plane path change" event.
Event Filter	O	Event filter as specified in 3GPP TS 23.501 [2]
EAS characteristics for ACR	O	Set of characteristics to determine required EAS as detailed in Table 8.5.3.2-2. Applicable for the "ACR monitoring" event and "ACR facilitation" event.
NOTE 1: Either UE ID or UE Group ID shall be provided if the Event ID(s) includes any of the "user plane path change", "ACR monitoring" and "ACR facilitation" events. UE ID or UE Group ID are not applicable to "ACT start/stop" event.		
NOTE 2: This IE shall be present if the Event ID(s) includes any of the "user plane path change", "ACR monitoring" and "ACR facilitation" events. This IE is not applicable to "ACT start/stop" event.		

8.6.3.3.3 ACR management event subscribe response

Table 8.6.3.3.3-1 describes the information elements for an ACR management event subscribe response from the EES to the EAS.

Table 8.6.3.3.3-1: ACR management event API subscribe response

Information element	Status	Description
Successful response (NOTE)	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time. If the Expiration time IE is not included, it indicates that the subscription never expires.
Failure response (NOTE)	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure
NOTE: One of these IEs shall be present in the message.		

8.6.3.3.4 ACR management event notification

Table 8.6.3.3.4-1 describes the information elements for an ACR management event notification from the EES to the EAS.

Table 8.6.3.3.4-1: ACR management event notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the EES for the request
List of event notifications	M	A list of event notifications for one or more UEs.
> Event ID	M	The event ID for which the notification is triggered: - user plane path change - ACR monitoring - ACR facilitation - ACT start/stop
> Event report (NOTE 1)	O	Event reporting information as specified in clause 5.2.8.3.1 of 3GPP TS 23.502 [3]
> Timestamp	O	The timestamp of each event report.
> EAS endpoint	O	The T-EAS endpoint shall be included for the "ACR monitoring" event and "ACR facilitation" event. In case of "ACT start/stop" event, the endpoint address of the EAS to or from which the ACT is needed to start/stop.
UEID (NOTE 2)	O	The identifier of the UE
NOTE 1: This IE shall be present if the Event ID(s) includes any of the "user plane path change", "ACR monitoring" and "ACR facilitation" events. This IE is not applicable to "ACT start/stop" event.		
NOTE 2: This IE shall be present only in case of "ACT start/stop" events.		

8.6.3.3.5 ACR management event subscription update request

Table 8.6.3.3.5-1 describes the information elements for an ACR management event subscribe request from the EAS to the EES.

Table 8.6.3.3.5-1: ACR management event subscription update request

Information element	Status	Description
Security credentials	M	Security credentials of the EAS
Subscription ID	M	The identifier of the subscription to be updated.
Event ID(s) (NOTE)	O	Event ID(s) as specified in 3GPP TS 23.501 [2]
Event Report (NOTE)	O	Event Reporting Information as specified in 3GPP TS 23.502 [3]
Type of subscription (NOTE)	O	Indicates Early and/or Late notification to inform if the notification needs to be received before and/or after UP path configuration.
Indication of EAS acknowledgement (NOTE)	O	This IE indicates the EES to include indication of "AF acknowledgement to be expected" within the AF request for subscribing UP path management events to 3GPP network and that the EAS will provide an acknowledgement as a response for the notifications of UP path management events to the EES.
Event Filter (NOTE)	O	Event filter as specified in 3GPP TS 23.501 [2]
EAS characteristics for ACR (NOTE)	O	Set of characteristics to determine required EAS as detailed in Table 8.5.3.2-2. Applicable for the "ACR monitoring" event and "ACR facilitation" event.
NOTE: At least one of these IEs shall be present in the message.		

8.6.3.3.6 ACR management event subscription update response

Table 8.6.3.3.6-1 describes the information elements for an ACR management event subscription update response from the EES to the EAS.

Table 8.6.3.3.6-1: ACR management event subscription update response

Information element	Status	Description
Successful response(NOTE 2)	O	Indicates that the subscription update request was successful.
> Expiration time (NOTE 1)	O	Indicates the expiration time of the updated subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response(NOTE 2)	O	Indicates that the subscription update request failed.
> Cause	O	Indicates the cause of subscription update request failure
NOTE 1: If the Expiry time IE is not included, it indicates that the subscription never expires.		
NOTE 2: One of these IEs shall be present in the message.		

8.6.3.3.7 ACR management event unsubscribe request

Table 8.6.3.3.7-1 describes the information elements for an ACR management event unsubscribe request from the EAS to the EES.

Table 8.6.3.3.7-1: ACR management event unsubscribe request

Information element	Status	Description
Security credentials	M	Security credentials of the EAS
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the EES for the request

8.6.3.3.8 ACR management event unsubscribe response

Table 8.6.3.3.8-1 describes the information elements for an ACR management event unsubscribe response from the EES to the EAS.

Table 8.6.3.3.8-1: ACR management event unsubscribe response

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

8.6.3.4 APIs

8.6.3.4.1 General

Table 8.6.3.4.1-1 illustrates the API for ACR management event.

Table 8.6.3.4.1-1: Eees_ACRManagementEvent API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_ACRManagementEvent	Subscribe	Subscribe/Notify	EAS
	Notify		
	UpdateSubscription		
	Unsubscribe		

8.6.3.4.2 Eees_ACRManagementEvent_Subscribe operation

API operation name: Eees_ACRManagementEvent_subscribe

Description: The consumer subscribes to receive an ACR management event.

Inputs: See clause 8.6.3.3.2.

Outputs: See clause 8.6.3.3.3.

See clause 8.6.3.2.2 for details of usage of this operation.

8.6.3.4.3 Eees_ACRManagementEvent_Notify operation

API operation name: Eees_ACRManagementEvent_Notify

Description: The consumer is notified of an event by the EES.

Inputs: See clause 8.6.3.3.4.

Outputs: None.

See clause 8.6.3.2.3 for details of usage of this operation.

8.6.3.4.4 Eees_ACRManagementEvent_UpdateSubscription operation

API operation name: Eees_ACRManagementEvent_UpdateSubscription

Description: The consumer updates an existing subscription for an ACR management event.

Inputs: See clause 8.6.3.3.5.

Outputs: See clause 8.6.3.3.6.

See clause 8.6.3.2.4 for details of usage of this operation.

8.6.3.4.5 Eees_ACRManagementEvent_Unsubscribe operation

API operation name: Eees_ACRManagementEvent_Unsubscribe

Description: The consumer unsubscribes for the previously subscribed events.

Inputs: See clause 8.6.3.3.7.

Outputs: See clause 8.6.3.3.8.

See clause 8.6.3.2.5 for details of usage of this operation.

8.6.4 AC information exposure API

8.6.4.1 General

AC information exposure enables EASs to obtain information about capabilities of ACs from the EESs. This information may facilitate communications between EASs and ACs, e.g. push notifications. The information shared is subject to access control as well as privacy and security mechanisms.

8.6.4.2 Procedures

8.6.4.2.1 General

8.6.4.2.2 Subscribe

Figure 8.6.4.2.2-1 illustrates the AC information subscription procedure between the EAS and the EES.

Pre-conditions:

1. The EAS is registered with the EES; and
2. The AC Profiles of the ACs on the UE are available at the EEC on the UE.

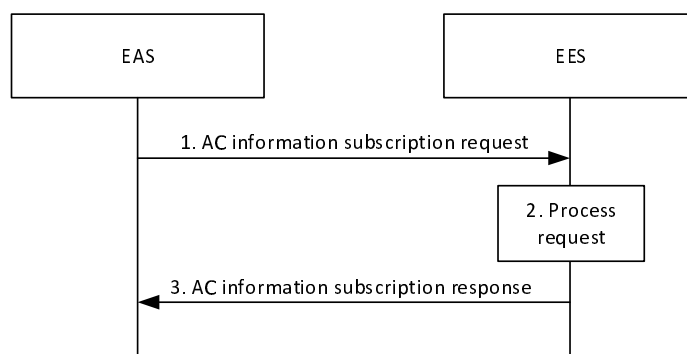


Figure 8.6.4.2.2-1: AC information subscription

1. The EAS sends an AC information subscription request to the EES. The request may contain filters to retrieve information about particular ACs e.g. AC profile parameters or parameter ranges to be matched, specific UE Identifiers, location ranges, etc.

NOTE: The trigger conditions of the AC information API (e.g. resource load predictive analytics) are up to service logic, which is out of scope of this specification.

2. Upon receiving the request from the EAS, the EES performs an authorization check to verify whether the EAS has authorization to perform the operation. The EES determines the matching AC information corresponding to the filter provided and composes a result. The EES stores the subscription information for future processing.

3. The EES sends an AC information subscription response to the EAS with the result composed in step 2.

8.6.4.2.3 Notify

Figure 8.6.4.2.3-1 illustrates the AC information notification procedure between the EES and the EAS.

Pre-conditions:

1. The EAS subscribed for AC information at the EES.

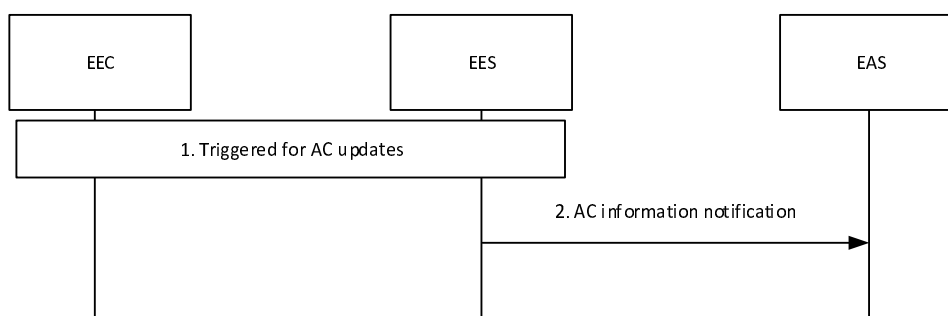


Figure 8.6.4.2.3-1: AC information notification

1. The EES is triggered for AC information updates, e.g. it receives an EEC registration request, it determines if it matches the filter provided by the EAS, e.g. if the AC Geographical Service Area is included in the EAS provided Geographical Service Area.
2. The EES sends an AC information notification to the EAS.

8.6.4.2.4 Subscription update

Figure 8.6.4.2.4-1 illustrates the AC information subscription update procedure between the EAS and the EES.

Pre-conditions:

1. The EAS has subscribed for AC information as described in clause 8.6.4.2.2.

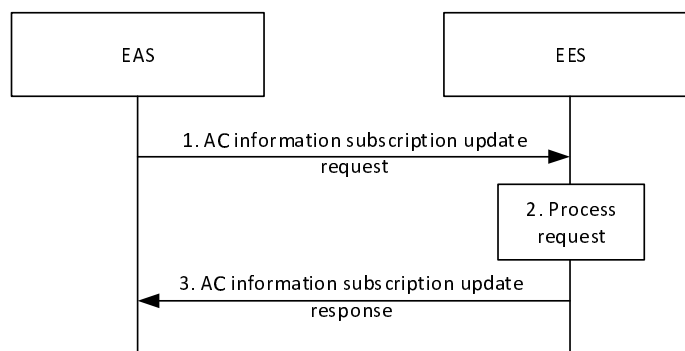


Figure 8.6.4.2.4-1: AC information subscription update

1. The EAS sends an AC information subscription update request to the EES. The request may contain updated filters to retrieve information about particular ACs e.g. AC profile parameters or parameter ranges to be matched, specific UE Identifiers, location ranges, etc.
2. Upon receiving the request from the EAS, the EES performs an authorization check to verify whether the EAS has authorization to perform the operation. If authorized, the EES updates the stored subscription information.

3. The EES sends an AC information subscription update response to the EAS.

8.6.4.2.5 Unsubscribe

Figure 8.6.4.2.5-1 illustrates the AC information unsubscribe procedure between the EAS and the EES.

Pre-conditions:

- 1. The EAS has subscribed for AC information as described in clause 8.6.4.2.2.

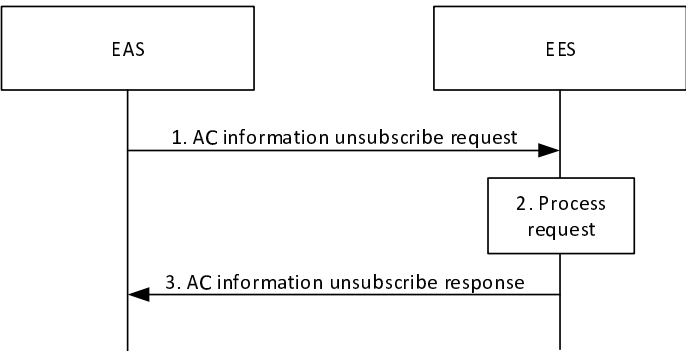


Figure 8.6.4.2.5-1: AC information unsubscribe

- 1. The EAS sends an AC information unsubscribe request to the EES.
- 2. Upon receiving the request from the EAS, the EES performs an authorization check to verify whether the EAS has authorization to perform the operation. If authorized, the EES cancels the subscription as requested in step 1.
- 3. The EES sends an AC information unsubscribe response to the EAS.

8.6.4.3 Information flows

8.6.4.3.1 General

8.6.4.3.2 AC information subscription request

Table 8.6.4.3.2-1 describes the information flow for an AC information subscription request from the EAS to the EES.

Table 8.6.4.3.2-1: AC information subscription request

Information element	Status	Description
EASID	M	The identifier of the EAS
Security credentials	M	Security credentials of the EAS
Subscription type	M	Choice of "One time" or "Event based" determining the type of processing requested
Notification Target Address	M	The Notification Target Address (e.g. URL) where the notifications destined for the EAS should be sent to.
Filters	O	List of characteristics for discovery purposes, as detailed in Table 8.6.4.3.2-2.
Event conditions	O	Parameters indicating event conditions e.g. number of notifications instances, subscription timeout, etc.

Table 8.6.4.3.2-2: Filters

Information element	Status	Description
ACID(s)	O	List of identities of AC(s) to be matched
UE ID(s)	O	List of UE identifiers to be matched
AC Type(s)	O	List of categories or types of ACs (e.g. V2X) to be matched
ECSP ID(s)	O	Identifier(s) for the ECSP associated with the EEC.
Operation Schedule	O	EAS operation schedule (e.g. time windows) to be matched
Geographical Service Area	O	EAS service area for identifying UEs with matching expected geographical location(s) (e.g. route). This geographic information can express a geographic point, polygon, route, signalling map, or waypoint set.
Topological Service Area	O	EAS service area for identifying UEs with matching expected topological location(s). See possible formats in Table 8.2.7-1.
Maximum AC Service KPIs (NOTE)	O	Maximum value for identifying the ACs to be matched. Both Minimum required AC Service KPIs and Expected AC Service KPIs from the AC Profiles provided during registration (Table 8.4.2.3.2-1) and/or discovery subscription (Table 8.5.3.4-1) need to be lower than this value.
Min AC Service KPIs (NOTE)	O	Minimum value for identifying the ACs to be matched. Both Minimum required AC Service KPIs and Expected AC Service KPIs from the AC Profiles provided during registration (Table 8.4.2.3.2-1) and/or discovery subscription (Table 8.5.3.4-1) need to be greater than this value.
UE location(s)	O	List of locations (e.g. routes) of the UE(s) for which the request applies
NOTE: Maximum and minimum AC Service KPIs values may be provided for any IEs from Table 8.2.3-1.		

8.6.4.3.3 AC information subscription response

Table 8.6.4.3.3-1 describes the information flow for the AC information subscription response from EAS to the EES.

Table 8.6.4.3.3-1: AC information subscription response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.6.4.3.4 AC information notification

Table 8.6.4.3.4-1 describes the information flow for an AC information notification from the EES to the EAS.

Table 8.6.4.3.4-1: AC information notification

Information element	Status	Description
Subscription Identifier	M	Subscription identifier for which the notification is generated.
List of clients	O	List of clients matched based on the given filtering criteria, with elements listed below
>AC Profile(s)	M	Profiles of ACs as described in Table 8.2.2-1.
>UE ID(s)	O	UE identifier for the UE hosting the AC
>UE location(s)	O	UE location for the UE hosting the AC

8.6.4.3.5 AC information subscription update request

Table 8.6.4.3.5-1 describes the information flow for an AC information subscription update request from the EAS to the EES.

Table 8.6.4.3.5-1: AC information subscription update request

Information element	Status	Description
Security credentials	M	Security credentials of the EAS
Subscription ID	M	Subscription identifier corresponding to the subscription.
Filter	O	List of characteristics for discovery purposes, as detailed in Table 8.6.4.3.2-2.
Event conditions	O	Parameters indicating event conditions e.g. number of notifications instances, subscription timeout, etc.

8.6.4.3.6 AC information subscription update response

Table 8.6.4.3.6-1 describes the information flow for the AC information subscription update response from EAS to the EES.

Table 8.6.4.3.6-1: AC information subscription update response

Information element	Status	Description
Successful response	O	Indicates that the subscription update request was successful.
Failure response	O	Indicates that the subscription update request failed.
> Cause	O	Indicates the cause of subscription update request failure

8.6.4.3.7 AC information unsubscribe request

Table 8.6.4.3.7-1 describes the information flow for an AC information unsubscribe request from the EAS to the EES.

Table 8.6.4.3.7-1: AC information unsubscribe request

Information element	Status	Description
Security credentials	M	Security credentials of the EAS
Subscription Identifier	M	Subscription identifier for the corresponding subscription request.

8.6.4.3.8 AC information unsubscribe response

Table 8.6.4.3.8-1 describes the information flow for the AC information unsubscribe response from EAS to the EES.

Table 8.6.4.3.8-1: AC information unsubscribe response

Information element	Status	Description
Successful response	O	Indicates that the unsubscribe request was successful.
Failure response	O	Indicates that the unsubscribe request failed.
> Cause	O	Indicates the cause of unsubscribe request failure

8.6.4.4 APIs

8.6.4.4.1 General

Table 8.6.4.4.1-1 illustrates the API for AC information exposure.

Table 8.6.4.4.1-1: Eees_AppClientInformation API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_AppClientInformation	Subscribe	Subscribe/Notify	EAS
	Notify		
	UpdateSubscription		
	Unsubscribe		

8.6.4.4.2 Eees_AppClientInformation_Subscribe operation

API operation name: Eees_AppClientInformation_subscribe

Description: The consumer subscribes to receive an AC information.

Inputs: See clause 8.6.4.3.2.

Outputs: See clause 8.6.4.3.3.

See clause 8.6.4.2.2 for details of usage of this operation.

8.6.4.4.3 Eees_AppClientInformation_Notify operation

API operation name: Eees_AppClientInformation_Notify

Description: The consumer is notified of an event by the EES.

Inputs: See clause 8.6.4.3.4.

Outputs: None.

See clause 8.6.4.2.3 for details of usage of this operation.

8.6.4.4.4 Eees_AppClientInformation_UpdateSubscription operation

API operation name: Eees_AppClientInformation_UpdateSubscription

Description: The consumer updates an existing subscription for AC information.

Inputs: See clause 8.6.4.3.5.

Outputs: See clause 8.6.4.3.6.

See clause 8.6.4.2.4 for details of usage of this operation.

8.6.4.4.5 Eees_AppClientInformation_Unsubscribe operation

API operation name: Eees_AppClientInformation_Unsubscribe

Description: The consumer unsubscribes for the previously subscribed events.

Inputs: See clause 8.6.4.3.7.

Outputs: See clause 8.6.4.3.8.

See clause 8.6.4.2.5 for details of usage of this operation.

8.6.5 UE Identifier API

8.6.5.1 General

EES exposes UE Identifier API to the EAS in order to provide an identifier uniquely identifying a UE. This API is used by an EAS to obtain the identifier of the UE if the EAS does not have it. This identifier, called UE ID, is used by the EAS to invoke capability APIs specific to UEs over EDGE-3. The UE ID is specific to the given EAS and it is represented as a GPSI assigned by the 3GPP Core Network.

8.6.5.2 Procedure

Figure 8.6.5.2-1 illustrates the interactions between the EES and the EAS.

Pre-conditions:

1. The EAS is authorized to discover and to use UE Identifier API provided by the EES.

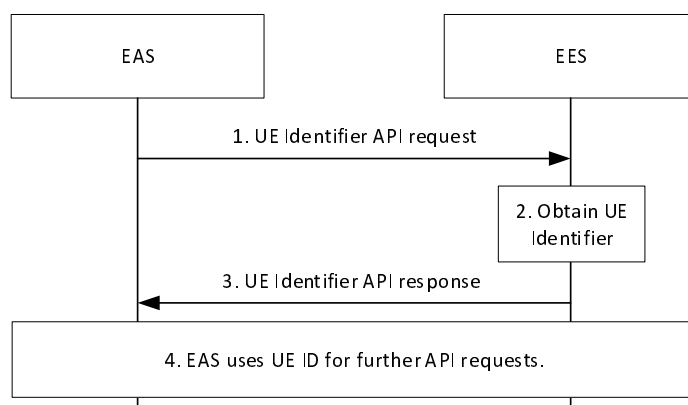


Figure 8.6.5.2-1: UE Identifier API

1. The EAS invokes UE Identifier API exposed by the EES.
2. The EES uses the received user information in the step 1 (e.g. IP address) and obtains the UE identifier by interacting with NEF as specified in clause 4.15.10 of 3GPP TS 23.502 [3].
3. The EES provides the obtained UE identifier as UE ID to the EAS.

Editor's note: [SA3] Whether and how user's consent is obtained to share the UE identifier with a particular EAS is SA3's responsibility.

4. The EAS uses the UE ID received in step 3 to invoke capability exposure API(s) provided by the EES over EDGE-3.

8.6.5.3 Information flows

8.6.5.3.1 General

The following information flows are specified for UE Identifier API:

- UE Identifier request and response.

8.6.5.3.2 UE Identifier API request

Table 8.6.5.3.2-1: UE Identifier API request

Information element	Status	Description
User information	M	Information about the User or UE available in the EAS, e.g. IP address.
EAS ID	M	Identifier of the EAS providing the application services.
EAS Provider ID	O	Identifier of the ASP that provides the EAS.
Security Credentials	M	Security credentials of the EAS.

Editor's Note: [SA3] Whether the EAS ID and the EAS Provider ID are part of the security credential is SA3's responsibility.

8.6.5.3.3 UE Identifier API response

Table 8.6.5.3.3-2: UE Identifier API response

Information element	Status	Description
Successful response	O	Indicates that the UE identifier request was successful.
> UE ID	M	Identifier uniquely identifying the UE.
Failure response	O	Indicates that the UE identifier request failed.
> Cause	O	Indicates the cause of UE identifier request failure

8.6.5.4 APIs

8.6.5.4.1 General

Table 8.6.5.4.1-1 illustrates the APIs for UE Identifier.

Table 8.6.5.4.1-1: Eees_UE_Identifier API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_UEIdentifier	Get	Request/Response	EAS

8.6.5.4.2 Eees_UEIdentifier_Get operation

API operation name: Eees_UEIdentifier_Get

Description: The consumer requests identifier of a UE.

Inputs: See clause 8.6.5.3.2.

Outputs: See clause 8.6.5.3.3.

See clause 8.6.5.2 for details of usage of this operation.

8.6.6 Session with QoS API

8.6.6.1 General

The EES exposes the Session with QoS API to the EAS in order to support the setup of a data session between AC and EAS with a specific QoS and the modification of the QoS of this data session.

The Session with QoS API exposed by the EES relies on the northbound Policy Authorization Service API exposed by the PCF as specified in 3GPP TS 23.502 [3] and 3GPP TS 23.503 [12], if the EES is connected to the PCF via the N5

reference point, or on the northbound AF Session with QoS Service API exposed by the NEF as specified in 3GPP TS 23.502 [3] and 3GPP TS 23.503 [12], if the EES is connected to the PCF via an NEF.

This API supports to apply the required QoS for both ongoing session and future session for a UE or a group of UEs.

The level of support of the Session with QoS API may change due to UE mobility between 5GC and EPC. E.g. QoS monitoring is only applicable in 5GC. If an EES exposes the Session with QoS API to EAS(s) for a UE, the EES monitors such changes and provides the available information to the EAS.

Alternatively to using the API described in the following clauses, the EAS may also act as an AF and directly access the 3GPP Core Network capabilities to request an AF session with QoS (see clause 8.7.2). For any data session between AC and EAS, the EAS shall use only one of these alternatives.

8.6.6.2 Procedures

8.6.6.2.1 General

8.6.6.2.2 Create a session

Figure 8.6.6.2.2-1 illustrates the session with QoS create operation between the EAS and the EES. It is used to request reservation of resources for a data session between AC and EAS with a specific QoS and to subscribe to certain session with QoS event notifications.

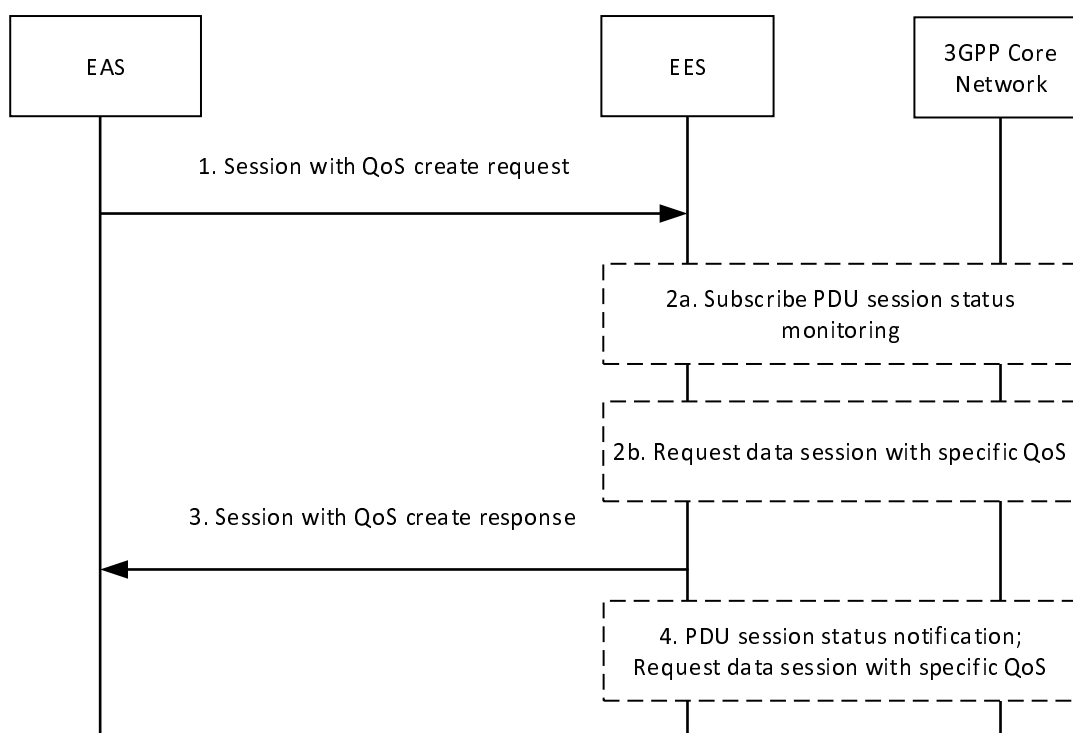


Figure 8.6.6.2.2-1: Session with QoS API: create operation

1. The EAS requests establishment of a data session between the AC and the EAS with a specific QoS (either QoS reference or bandwidth). If the data session can adjust to different QoS parameter combinations, the request may include a list of alternative QoS references in a priority order. The EAS shall include the UE's IP address, UE ID or UE Group ID, the DNN and S-NSSAI used for the data session between AC and EAS. With the same request the EAS subscribes to receive certain session with QoS event notifications (e.g. notifications related to QoS monitoring, usage monitoring for sponsored data connectivity and/or QoS targets can no longer (or can again) be fulfilled).
2. The EES checks if the EAS is authorized for this operation for the UE. If authorized, then the following services of 3GPP CN may be used by the EES:

- a. the EES invokes the Event Monitoring service for PDU session status with the 3GPP Core Network, as described in 3GPP TS 23.502 [3].
- b. the EES invokes the Policy Authorization Create service or the AF Session with QoS service with the 3GPP Core Network (PCF or NEF, respectively) as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3], providing the specific QoS (QoS reference or bandwidth) to the PCF as described in 3GPP TS 23.503 [12], clause 6.1.3.22. Additionally, the EES may subscribe to notifications of resource allocation outcome and to other events described in clause 6.1.3.18 of 3GPP TS 23.503 [12], e.g. notifications of when the QoS targets can no longer (or can again) be fulfilled.

The usage of step 2a and step 2b is as follows:

- If the request is for a group of UEs identified by the UE Group ID or for a single UE identified by the UE ID, then EES executes step 2a. If UE (single UE or UE group member) already has ongoing PDU session, then UE IP address is retrieved in step 2a. Further the EES executes step 2b; otherwise the EES waits for further notification for PDU session status in step 4.
 - If the request is for a single UE identified by the IP address, then EES executes step 2b.
3. If the operation in step 2 is successful, the EES responds with a Context ID and a Result. The Context ID is to be used by the EAS for further requests (e.g. session with QoS update requests) pertaining to the same UE. If the EAS is not authorized or any other failure happens during the operation, the EES provides a rejection response with cause information.
 4. When the EES receives the corresponding UE IP address for the single UE or UE group member from the PDU session status notification sent by the 3GPP Core Network, the EES requests data session with specific QoS as described in step 2b.

NOTE: The EES will report the resource allocation outcome, e.g. the successful allocation of the Service Data Flow(s) related to the data session, with a separate session with QoS notify operation (see TS 23.503 [12], clause 6.1.3.18).

8.6.6.2.3 Update a session

Figure 8.6.6.2.3-1 illustrates the session with QoS update request operation between the EAS and the EES. It is used to request a modification of the QoS of the data session between AC and EAS.

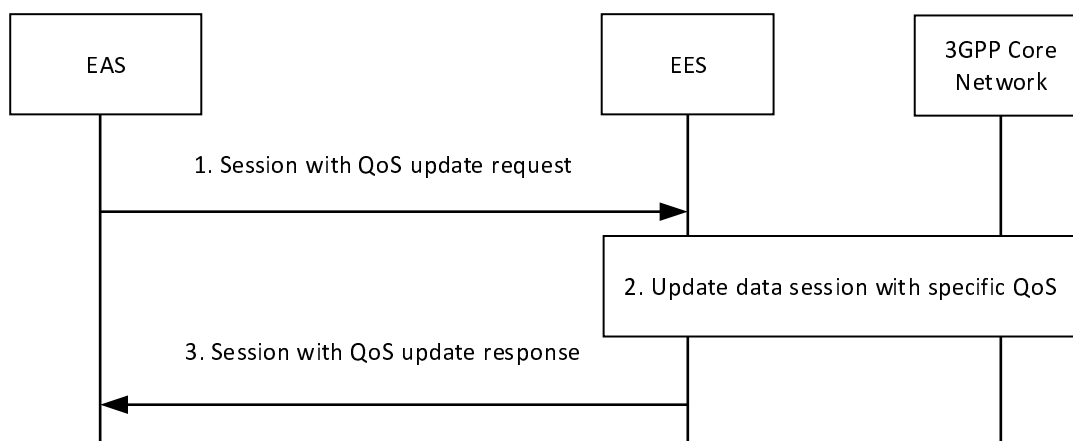


Figure 8.6.6.2.3-1: Session with QoS API: update operation

1. The EAS requests a modification of the QoS of the data session between the AC and the EAS, e.g. by including a different QoS reference or different bandwidth value. The EAS shall include the Context ID.

The EAS may also request a modification of the event monitoring by subscribing to new events and updating or removing subscriptions to existing events.

2. The EES checks if there is a context for the Context ID available and whether the EAS is authorized for this operation. If yes and the UE IP address is known by the EES, the EES invokes the Policy Authorization Update service or AF Session with QoS Update service with the 3GPP Core Network (PCF or NEF, respectively) as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3], providing the updated information to the PCF or NEF, respectively. The EES may subscribe to additional events or unsubscribe to certain events, if necessary.
3. If the operation is successful, the EES responds with a Context ID and a Result. If the EAS is not authorized or any other failure happens during the operation, the EES provides a rejection response with cause information.

NOTE: The EES will report the resource allocation outcome, e.g. the successful modification of the Service Data Flow(s) related to the data session, with a separate session with QoS notify operation (see 3GPP TS 23.503 [12], clause 6.1.3.18).

8.6.6.2.4 Revoke a session

Figure 8.6.6.2.4-1 illustrates the session with QoS revoke operation between the EAS and the EES. It is used to revoke the data session between AC and EAS with a specific QoS and to unsubscribe to the related session with QoS event notifications.

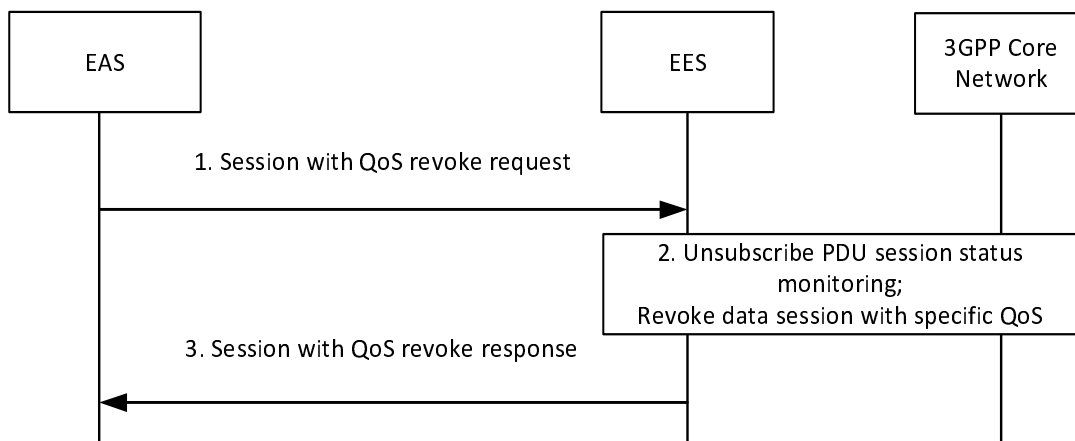


Figure 8.6.6.2.4-1: Session with QoS API: revoke operation

1. The EAS requests a revoke of the data session with QoS between the AC and the EAS. The EAS shall include the Context ID.
2. The EES checks if there is a context for the Context ID available and whether the EAS is authorized for this operation. If yes, then the EES unsubscribes from the PDU session status monitoring (if applicable) and invokes the Policy Authorization Delete service or AF Session with QoS Revoke service with the 3GPP Core Network (PCF or NEF, respectively) as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3]. This deletes the application session context at the PCF or NEF and removes the subscription to any session with QoS event notifications.
3. If the operation is successful, the EES responds with a Context ID and a Result. If the EAS is not authorized or any other failure happens during the operation, the EES provides a rejection response with cause information.

8.6.6.2.5 Notify

Figure 8.6.6.2.5-1 illustrates the notify operation between the EES and the EAS for session with QoS event notifications.

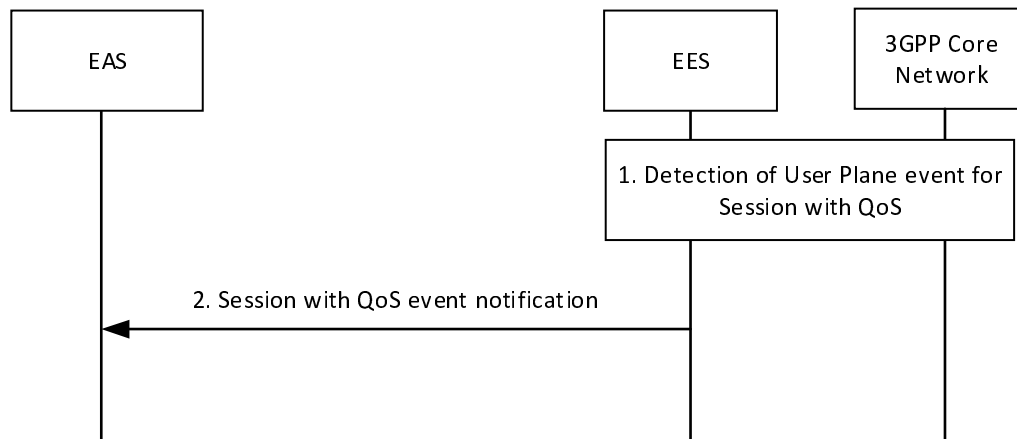


Figure 8.6.6.2.5-1: Session with QoS API: notify operation

1. The EES detects a user plane event associated with the established session (i.e. it receives a Policy Authorization Notify operation from the PCC or an AF Session with QoS Notify operation from the NEF as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3]). The EES determines to notify the session with QoS event notification information (e.g., resource allocation outcome or information that the QoS targets can no longer (or can again) be fulfilled) to the EASs which have subscribed to the session with QoS event notification.
2. The EES sends a session with QoS event notification to the EAS. The EES includes the session with QoS event notification information of the UE.

8.6.6.3 Information flows

8.6.6.3.1 General

The following information flows are specified for Session with QoS API:

- Session with QoS create request and response;
- Session with QoS update request and response;
- Session with QoS revoke request and response; and
- Session with QoS event notification.

8.6.6.3.2 Session with QoS create request

Table 8.6.6.3.2-1 describes the information elements for a Session with QoS create request from the EAS to the EES.

Table 8.6.6.3.2-1: Session with QoS create request

Information element	Status	Description
EASID	M	The identifier of the EAS
Security credentials	M	Security credentials of the EAS
UE IP address (NOTE 1)	O	The UE IP address.
UE ID (NOTE 1)	O	The identifier of the UE (i.e. GPSI)
UE Group ID (NOTE 1)	O	Identifies a group of UEs (i.e. internal group ID or external group ID)
IP flow description	M	The IP flow description for the application traffic.
Requested QoS reference (NOTE 2)	O	Refers to pre-defined QoS information for the data session between AC and EAS (NOTE 3).
List of alternative QoS references	O	A list of alternative QoS references, referring to pre-defined QoS information for the data session between AC and EAS and containing one or more QoS reference parameters in a prioritized order (NOTE 3).
Event list	O	A list of associated events to which the EAS subscribes (see 3GPP TS 23.503 [12], clause 6.1.3.18).
> Event specific data	O	For usage monitoring: the sponsoring information (sponsor id, ASP id). For QoS monitoring: Target of monitoring (DL, UL or roundtrip packet delay).
> Frequency of reporting	O	The reporting frequency (e.g. event triggered) and additional related data (e.g. threshold, minimum waiting time) as described in clause 6.1.3.21 of 3GPP TS 23.503 [12], applicable for QoS monitoring event.
Notification Target Address	M	The Notification Target Address (e.g. URL) where the notifications destined for the EAS should be sent to.
DNN	O	DNN for the data session between AC and EAS
S-NSSAI	O	S-NSSAI for the data session between AC and EAS
Requested bandwidth (NOTE 2)	O	Bandwidth requested for the data session between AC and EAS
NOTE 1: Only one of UE IP address, UE ID or UE Group ID shall be provided. NOTE 2: Only one of requested QoS reference or requested bandwidth shall be provided. NOTE 3: The pre-defined QoS information may be configured in the EES or in the 3GPP Core Network (see 3GPP TS 23.503 [12], clause 6.1.3.22).		

8.6.6.3.3 Session with QoS create response

Table 8.6.6.3.3-1 describes the information elements for a Session with QoS create response from the EES to the EAS.

Table 8.6.6.3.3-1: Session with QoS create response

Information element	Status	Description
Successful response	O	Indicates that the Session with QoS create request was successful.
> Context ID	M	Context identifier corresponding to the information stored for the request in the EES
Failure response	O	Indicates that the Session with QoS create request failed.
> Cause	O	Indicates the cause of Session with QoS create request failure

8.6.6.3.4 Session with QoS update request

Table 8.6.6.3.4-1 describes the information elements for a Session with QoS update request from the EAS to the EES.

Table 8.6.6.3.4-1: Session with QoS update request

Information element	Status	Description
Security credentials	M	Security credentials of the EAS
Context ID	M	Context identifier corresponding to the information stored for the request in the EES.
Requested QoS reference (NOTE 1)	O	Refers to pre-defined QoS information for the data session between AC and EAS (NOTE 2).
List of alternative QoS references	O	A list of alternative QoS references, referring to pre-defined QoS information for the data session between AC and EAS and containing one or more QoS reference parameters in a prioritized order (NOTE 2).
Event list	O	A list of associated events to which the EAS subscribes (see 3GPP TS 23.503 [12], clause 6.1.3.18).
> Event specific data	O	For usage monitoring: the sponsoring information (sponsor id, ASP id). For QoS monitoring: Target of monitoring (DL, UL or roundtrip packet delay).
> Frequency of reporting	O	The reporting frequency (e.g. event triggered) and additional related data (e.g. threshold, minimum waiting time) as described in clause 6.1.3.21 of 3GPP TS 23.503 [12], applicable for QoS monitoring event.
Requested bandwidth (NOTE 1)	O	Bandwidth requested for the data session between AC and EAS
NOTE 1: Only one of requested QoS reference or requested bandwidth shall be provided. NOTE 2: The pre-defined QoS information may be configured in the EES or in the 3GPP Core Network (see 3GPP TS 23.503 [12], clause 6.1.3.22).		

8.6.6.3.5 Session with QoS update response

Table 8.6.6.3.5-1 describes the information elements for a Session with QoS update response from the EES to the EAS.

Table 8.6.6.3.5-1: Session with QoS update response

Information element	Status	Description
Successful response	O	Indicates that the Session with QoS update request was successful.
Failure response	O	Indicates that the Session with QoS update request failed.
> Cause	O	Indicates the cause of Session with QoS update request failure

8.6.6.3.6 Session with QoS revoke request

Table 8.6.6.3.6-1 describes the information elements for a Session with QoS revoke request from the EAS to the EES.

Table 8.6.6.3.6-1: Session with QoS event API revoke request

Information element	Status	Description
Security credentials	M	Security credentials of the EAS
Context ID	M	Context identifier corresponding to the information stored for the request in the EES

8.6.6.3.7 Session with QoS revoke response

Table 8.6.6.3.7-1 describes the information elements for a Session with QoS revoke response from the EES to the EAS.

Table 8.6.6.3.7-1: Session with QoS revoke response

Information element	Status	Description
Successful response	O	Indicates that the Session with QoS revoke request was successful.
Failure response	O	Indicates that the Session with QoS revoke request failed.
> Cause	O	Indicates the cause of Session with QoS revoke request failure

8.6.6.3.8 Session with QoS event notification

Table 8.6.6.3.8-1 describes the information elements for a Session with QoS event notification from the EES to the EAS.

Table 8.6.6.3.8-1: Session with QoS event notification

Information element	Status	Description
Context ID	M	Context identifier corresponding to the information stored in the EES during the initial session with QoS create request.
Event report (NOTE)	M	Event reporting information as specified in clause 6.1.3.18 of 3GPP TS 23.503 [12].
NOTE: Only the following events are applicable: - Reporting Usage for Sponsored Data Connectivity - Service Data Flow deactivation - Resource allocation outcome - QoS targets can no longer (or can again) be fulfilled - QoS Monitoring parameters		

8.6.6.4 APIs

8.6.6.4.1 General

Table 8.6.6.4.1-1 illustrates the API for Session with QoS.

Table 8.6.6.4.1-1: Eees_SessionWithQoS API

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_SessionWithQoS	Create	Request/Response	EAS
	Update		
	Revoke		
	Notify	Subscribe/Notify (NOTE)	EAS
NOTE: The Subscribe operation is embedded in the Request operation of the Create and Update API operation.			

8.6.6.4.2 Eees_SessionWithQoS_Create operation

API operation name: Eees_SessionWithQoS_Create

Description: The consumer requests a data session with the UE with a specific QoS and may also subscribe to certain event notifications related to the user plane traffic.

Inputs: See clause 8.6.6.3.2.

Outputs: See clause 8.6.6.3.3.

See clause 8.6.6.2.2 for details of usage of this operation.

8.6.6.4.3 Eees_SessionWithQoS_Update operation

API operation name: Eees_SessionWithQoS_Update

Description: The consumer requests a modification of the QoS of the data session with the UE and may also update event notifications related to the user plane traffic.

Inputs: See clause 8.6.6.3.4.

Outputs: See clause 8.6.6.3.5.

See clause 8.6.6.2.3 for details of usage of this operation.

8.6.6.4.4 Eees_SessionWithQoS_Revoke operation

API operation name: Eees_SessionWithQoS_Revoke

Description: The consumer requests a revoke of the data session with QoS with the UE and unsubscribes to all related event notifications.

Inputs: See clause 8.6.6.3.6.

Outputs: See clause 8.6.6.3.7.

See clause 8.6.6.2.4 for details of usage of this operation.

8.6.6.4.5 Eees_SessionWithQoS_Notify operation

API operation name: Eees_SessionWithQoS_Notify

Description: The consumer is notified by the EES of an event related to the user plane traffic.

Inputs: See clause 8.6.6.3.8.

Outputs: None.

See clause 8.6.6.2.5 for details of usage of this operation.

8.7 Network capability exposure to EAS

8.7.1 General

The network capability exposure to EAS(s) depends on the deployment scenarios and the business relationship of the ASP/ECSP with the PLMN operator. The following mechanisms are supported:

- Direct network capability exposure.
- Network capability exposure via EES.

8.7.2 Direct network capability exposure

The EAS(s) (acting as trusted or untrusted AF) may directly access the 3GPP Core Network capabilities as specified in 3GPP TS 23.501 [2] and 3GPP TS 23.682 [17].

8.7.3 Network capability exposure via EES

The EES may re-expose the network capabilities of the 3GPP core network to the EAS(s) as per the CAPIF architecture specified in 3GPP TS 23.222 [6].

Depending on the deployment models (centralized or distributed) employed,

- the EES assumes the role of the API exposing function (may also acts as the API topology hiding entry) as described in 3GPP TS 23.222 [6]; and
- the EAS assumes the role of an API invoker.

If CAPIF is supported, the EAS interacts with the CAPIF core function and the EES. The EES may further interact with 3GPP northbound service API provider (e.g. SCEF/NEF/SCEF+NEF) or directly with 3GPP core network entities (e.g. PCF) to satisfy the service API invocation requests from the EASs.

The EES may expose the network capabilities of the 3GPP Core Networks to the EAS(s) by supporting the functionalities of 3GPP northbound service API provider (e.g. SCEF, NEF, SCEF+NEF).

NOTE: Details of how to select a proper 3GPP network exposure function (e.g. selecting NEF, SCEF, or SCEF+NEF) for the UE(s) is outside scope of this specification.

8.8 Service continuity

8.8.1 General

8.8.1.1 High level overview

When a UE moves to a new location, different EASs can be more suitable for serving the ACs in the UE. Such transitions can result from a non-mobility event also, requiring support from the enabling layer to maintain the continuity of the service.

This clause describes the features that support service continuity for ACs in the UE to minimize service interruption while replacing the S-EAS, with a T-EAS.

Generally, one AC on the UE has one associated application context at the S-EAS. To support service continuity, this application context is transferred from the S-EAS to a T-EAS.

The capabilities for supporting service continuity provided at the Edge Enabler Layer may consider various application layer scenarios in which there may be involvement of AC and one or more EAS(s).

Following intra-EDN, inter-EDN and LADN (overlapping LADN service areas) related scenarios are supported for service continuity:

- UE mobility, including predictive or expected UE mobility;
- Overload situations in S-EAS or EDN; and
- Maintenance aspects such as graceful shutdown of an EAS.

NOTE 1: The scenarios which require ACR for service continuity, cannot use non-overlapping LADNs.

To support the need of ACR, following entity roles are identified:

- detection entity, detecting or predicting the need of ACR;
- decision-making entity, deciding that the ACR is required; and
- execution entity, executing ACR.

A detection entity detects the probable need for ACR by monitoring various aspects, such as UE's location or predicted/expected UE location and indicates to the decision-making entity to determine if the ACR is required. The EEC, EES and EAS can potentially perform the detection role:

A decision-making entity determines that ACR is required and instructs the execution entity to perform ACR.

An execution entity performs ACR as and when instructed by the decision-making entity.

NOTE 2: After a decision that another EAS is to serve the UE, the S-EAS can decide if the existing Application Context is transferred to the new EAS.

The EAS may utilize the following capabilities provided by the EES for supporting service continuity at the application layer:

- Subscribe to service continuity related events and receive corresponding notifications;
- Discover the T-EAS; and
- ACR from a S-EAS to a T-EAS.

The EES can utilize the following capabilities provided by the ECS for supporting service continuity at the application layer:

- Retrieve the T-EES.

The EEC may determine if the ACR is required by detecting that the UE moved or is predicted or expected to move outside the service area (see clause 7.3.3). The service area can be provided to the EEC by either the ECS during Service Provisioning or EES during EAS Discovery. For the PDU Session of SSC mode 3, if the UE receives PDU Session Modification Command as specified in clause 4.3.5.2 of 3GPP TS 23.502 [3], the EEC may determine that the ACR is required. For IPv6 multi-homed PDU Session of SSC mode 3, the EEC may determine that ACR is required if the UE is notified of the existence and availability of a new IPv6 prefix as specified in clause 4.3.5.3 of 3GPP TS 23.502 [3].

NOTE 3: For IPv6 multi-homed PDU Session of SSC mode 3, the EEC can be aware of the notification about the IPv6 prefix configuration due to change of PSA UPF based on the UE implementation.

After successful ACR:

- The EES is informed of the completion by the EAS; and
- The EEC is informed of the completion by the EES.

In general, a number of steps are required in order to perform ACR. The potential roles of an edge enablement layer in ACR include:

- providing detection events;
- selecting the T-EAS(s); and
- supporting the transfer of the application context from the S-EAS(s) to the T-EAS(s).

If the UE is connected to the 5GC, the EES/EAS acting as AF may utilize AF traffic influence functionality from the 3GPP CN as specified in 3GPP TS 23.502 [3].

A high level overview of ACR is illustrated in Figure 8.8.1.1-1.

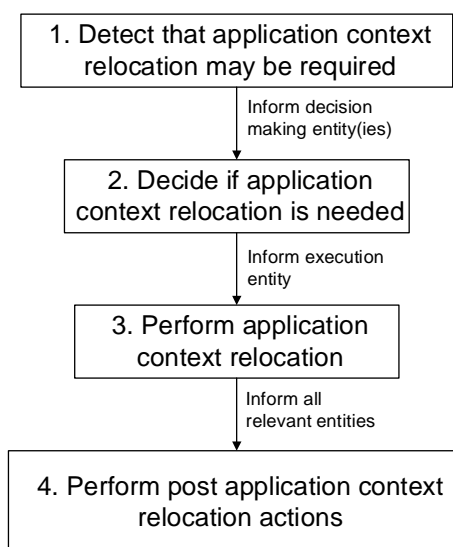


Figure 8.8.1.1-1: High level overview of ACR

ACR can be performed for service continuity planning, which means that the first three steps in Figure 8.8.1.1-1 detection, decision and execution, are performed as defined in clause 8.8.1.2, e.g. when the UE is predicted to move outside the service area of the serving EAS. In such a case the T-EAS is to service the UE when it moves to the expected location.

EES can handle multiple ACR requests simultaneously. When there are multiple simultaneous ACR, the ACR shall be uniquely identified by ACID, EEC ID (or UE ID), S-EAS endpoint and T-EAS endpoint.

8.8.1.2 ACR with service continuity planning

Service continuity planning is an Edge Enabler Layer value-add feature of providing support for seamless service continuity, when information about planned, projected, or anticipated behaviour is available at EESs or provided by EECs.

To implement this functionality an EES may utilize:

- information provided by the EEC e.g., AC Schedule, Expected AC Geographical Service Area, Expected Service KPIs, Preferred ECSP list; and
- 3GPP core network capabilities utilized by EES as described in clause 8.10.3.

In service continuity planning, the Application Context may be duplicated and sent from the S-EAS to the T-EAS before the UE moves to the expected location. In this case, the Application Contexts in S-EAS and T-EAS are synchronized when the Application Context is updated until the AC connects to the T-EAS.

NOTE 1: The information elements of the Application Context and how the Application Context is synchronized between the S-EAS and the T-EAS is up to implementation of the application.

NOTE 2: In the case of EELManagedACR, the Application Context synchronization is accomplished using the same mechanism as when transferring the context from the S-EES to the T-EES.

For additional details on service continuity planning for ACR, see clauses 8.8.2.2, 8.8.2.3, 8.8.2.4, 8.8.2.5 and 8.8.2.6.

8.8.1.3 Unused contexts handling during ACR including service continuity planning

The interval between ACT initiation and ACR status update message from EAS to EES (i.e. taking the context into use) can be significant (e.g. in the predicted case). During this interval, the following events are possible:

- a) The UE remains communicating with the S-EAS, e.g. the UE does not move to the service area of the T-EAS; or
- b) The UE moves to a service area served by a different T-EAS (other than the T-EAS towards which the ACR was initiated).

For the ACRs initiated by the EEC, in case of events a) and b) the EEC should re-send an ACR request with the information of the current ACR and the updated information as described in clause 8.8.3.4 and defined in clause 8.8.4.4. For a) if the action is initiation the EEC sets T-EAS endpoint under ACR initiation action to indicate the S-EAS. For b) if the action is initiation the UE sets T-EAS endpoint under ACR initiation action to the new T-EAS.

NOTE: Timeouts if required for discarding unused contexts for ACR scenarios can be specified in stage 3.

8.8.2 Scenarios

8.8.2.1 General

ACR functionality can be implemented flexibly, and may be focused either in the EEC or in the EAS/EES. The scenarios in this clause are different with regards to

- a) whether the EEC is involved in the detection phase and decision phase or detection and decision involve the S-EAS or S-EES only;
- b) whether T-EAS discovery is performed between EEC and T-EES or between S-EES and T-EES;

- c) whether the EEC sends an Application Context Relocation Request towards the S-EES, the T-EES or none at all; and
- d) whether the Application Context is pushed from the S-EAS to the T-EAS or pulled by the T-EAS from S-EAS.

Generally, AC, EEC, EES and EAS implementations will support only a subset of these scenarios; therefore, during EAS discovery and T-EAS discovery the S-EES and T-EES shall take the ACR scenarios supported by the AC and EEC and any preferences indicated by the EEC for specific ACR scenarios into account when identifying the EAS(s) for the EAS discovery response, as specified in clause 8.5.2.2 and clause 8.8.3.2, or for the EAS discovery notification, as specified in clause 8.5.2.3.3.

Furthermore, when the EEC performs EAS discovery or T-EAS discovery, the EES or T-EES shall inform the EEC about the ACR scenarios which are supported by the EAS or T-EAS, respectively.

The EEC shall take the information about supported ACR scenarios provided by the ECS, S-EES and T-EES into account when selecting an EES for EAS discovery or T-EAS discovery, respectively, and when selecting an EAS for edge services.

For clarity of description, scenarios in clauses 8.8.2.2, 8.8.2.3, 8.8.2.4, 8.8.2.5 and 8.8.2.6 describe the relocation of a single application context to a new EAS. Multiple ACs can be active in the UE and relocation can be executed for each AC (or group of ACs) that requires service continuity.

For each of the scenarios in clauses 8.8.2.2, 8.8.2.3, 8.8.2.4, 8.8.2.5 and 8.8.2.6, ACR for one or more ACs can result in the same EEC receiving services from more than one EES, which have the registration for the required EASs that can serve the ACs. In scenarios described in clause 8.8.2.4 and clause 8.8.2.5, a successful EEC context relocation procedure enables the EEC to become implicitly registered to the target EES without the EEC sending an EEC registration request.

Editor's note: whether the scenarios are overlapping and how to solve any co-existence issues are FFS.

8.8.2.2 Initiation by EEC using regular EAS Discovery

In this scenario, ACR is a result of the UE moving to, or the UE expecting to move to, a new location which is outside the service area of the serving EAS. The EEC is triggered as a result of the UE's movement as described in 8.8.1.1.

This scenario is based on Service Provisioning (as specified in clause 8.3) and EAS Discovery (as specified in clause 8.5) procedures to discover the T-EES and EAS that shall serve the AC as a result of the UE's new location, and that shall receive the Application Context from the serving EAS.

This scenario relies on an interface between the EEC and AC over EDGE-5, which is out of the scope of this specification.

Pre-conditions:

1. The AC in the UE already has a connection to a corresponding S-EAS;
2. The preconditions listed in clause 8.3.3.2.2 with regards to the EEC are fulfilled; and
3. The EEC is triggered when it obtains the UE's new location or is triggered by another entity such as an ECS notification

NOTE 1: This scenario is applicable only for an Edge-aware AC and EAS.

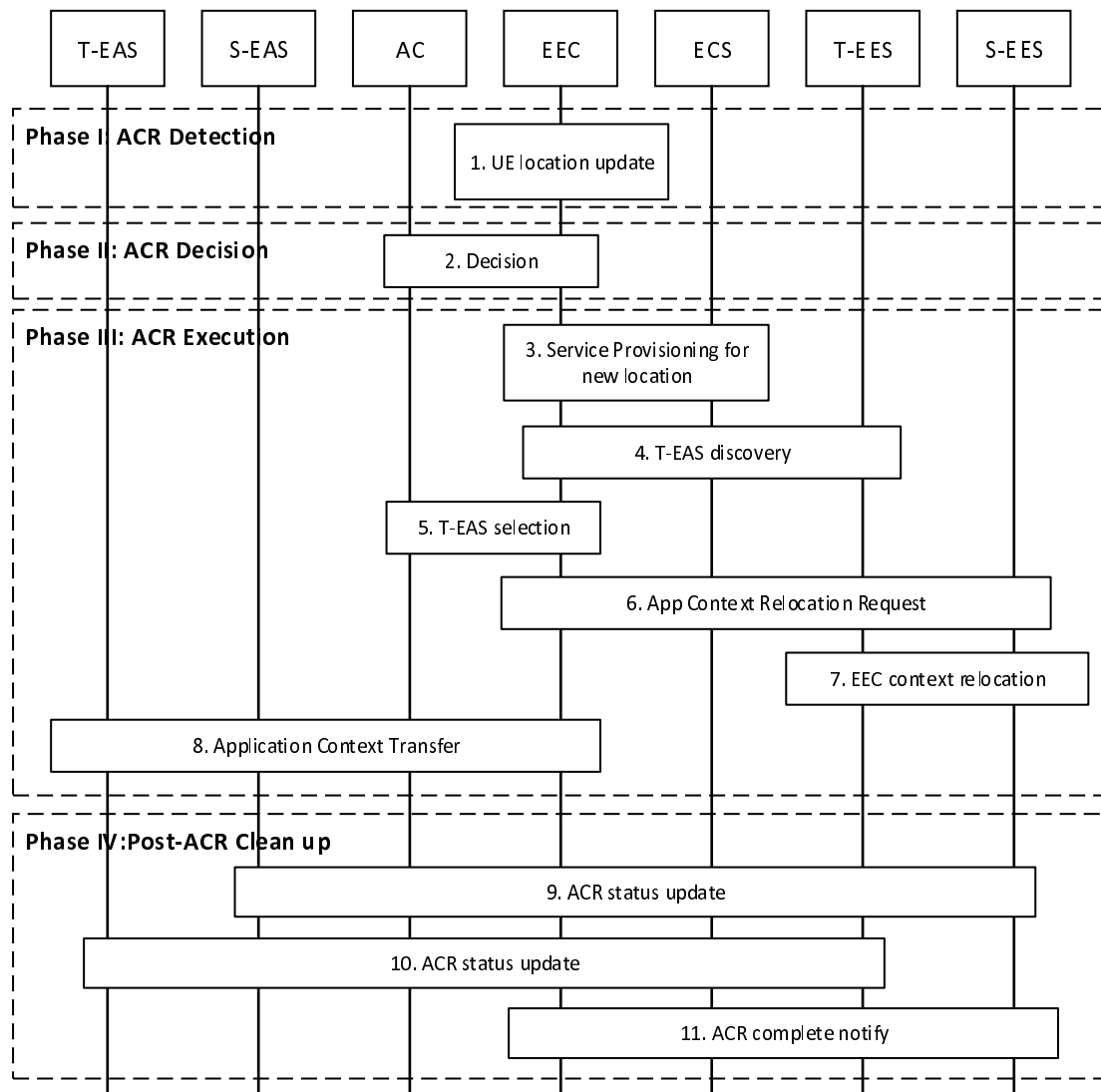


Figure 8.8.2.2-1: ACR initiated by the EEC and AC

Phase I: ACR Detection

1. The EEC detects the UE location update as a result of a UE mobility event and is provided with the UE's new location as described in clause 8.8.1.1. The EEC can also detect an expected or predicted UE location in the future as described in clause 8.8.1.1.

NOTE 2: If the EEC is triggered by an external entity such as by a notification from the ECS, a list of new EESs (to be used as T-EESs) is provided by that notification and step 3 below is skipped.

Phase II: ACR Decision

2. Either the AC or the EEC makes the decision to perform the ACR.

NOTE 3: Which applications require ACR can be decided based on the application profile, e.g. requirement of service continuity of the application.

If the change in UE's location does not trigger a need to change the serving EAS, steps 3. onwards are skipped. The EEC remains connected to the serving EES(s) and the AC remains connected to its corresponding serving EAS.

Phase III: ACR Execution

3. The EEC performs Service Provisioning (as specified in clause 8.3) for all active applications that require ACR. Since the location of the UE has changed, the Service Provisioning procedure results in a list of T-EESs that are relevant to the supplied applications and the new location of the UE. When in step 1 the ACR for service continuity planning is triggered, then the Connectivity information and UE Location in the Service Provisioning procedure (as specified in clause 8.3) contains the expected Connectivity information and expected UE Location.
4. The EEC performs EAS discovery (as specified in clause 8.5) for the desired T-EASs by querying the T-EESs that were established in step 3 (or provided in the notification from the ECS – if it was the trigger). If EEC registration configuration for the EESs established in step 2 indicates that EEC registration is required, the EEC performs EEC registration with the EESs (as specified in clause 8.4.2.2.2) before sending the EAS discovery request. Step 5 is skipped if EAS discovery procedure results in only one discovered T-EAS.
5. The AC and EEC select the T-EAS to be used for the application traffic.

NOTE 4: Several EEC registrations with different EESs may result from T-EAS discovery process during a single ACR operation.

6. The EEC performs ACR launching procedure (as described in clause 8.8.3.4) to the S-EES with the ACR action indicating ACR initiation and the corresponding ACR initiation data (without the need to notify the EAS). The S-EES may apply the AF traffic influence with the N6 routing information of the T-EAS in the 3GPP Core Network (if applicable), as described in clause 8.8.3.4. If the EEC has not subscribed to receive ACR information notifications for ACR complete events from the S-EES, the EEC subscribes for the notifications as described in clause 8.8.3.5.2.
7. If the T-EES is different than the S-EES and the EEC Context at the S-EES is not stale, the S-EES initiates EEC Context Push relocation with the T-EES as described in clause 8.9.2.3. Otherwise, if the T-EES is the same as the S-EES, EEC Context Push relocation is skipped.
8. The AC is triggered by the EEC to start ACT. The AC decides to initiate the transfer of application context from the S-EAS to the T-EAS. There may be different ways of transferring context and they are all outside the scope of this specification.

When in step 1 the ACR for service continuity planning has been triggered, the AC connects to the T-EAS when the UE moves to the predicted location. Otherwise, the rest of this step is skipped.

After the ACT is completed, the AC remains connected to the T-EAS and disconnects from the S-EAS; the EEC is informed of the completion.

NOTE 5: Whether and how the AC initiates the ACT is out of scope of the present document

When in step 1 the ACR has been triggered for service continuity planning, if the UE does not move to the expected/predicted location the EEC does not connect to T-EES, the AC does not connect to the T-EAS. Post-ACR Clean-up is skipped.

NOTE 6: The S-EAS or T-EAS can further decide to terminate the ACR, and the T-EAS can discard the application context based on information received from EEL and/or other methods (e.g. monitoring the location of the UE). It is up to the implementation of the S-EAS and T-EAS whether and how to make such a decision.

NOTE 7: It is out of scope of this specification how the AC informs the S-EAS and T-EAS that ACT was part of service continuity planning. When in step 1 the ACR for service continuity planning is triggered, Post-ACR Clean up is performed after the UE moves to the predicted location.

Phase IV: Post-ACR Clean up

9. The S-EAS sends the ACR status update message to the S-EES as specified in clause 8.8.3.8.
10. The T-EAS sends the ACR status update message to the T-EES as specified in clause 8.8.3.8. If the status indicates a successful ACT, and that the EEC Context relocation procedure was attempted but failed, then the T-EES indicates the failure to the T-EAS with the ACR status update response.

NOTE 8: If the EDGE-3 subscription initialization result indicates failure, then the EAS can perform the required EDGE-3 subscriptions at the T-EES.

NOTE 9: Steps 9 and 10 can occur in any order.

11. If the status in step 9 indicates a successful ACT, the S-EES sends the ACR information notification (ACR complete) message to the EEC to confirm that the ACR has completed as specified in clause 8.8.3.5.3. If the EEC Context relocation procedure was attempted, then the notification includes EEC context relocation status IE, indicating the result of the EEC context relocation procedure. If the EEC context relocation status indicates that the EEC context relocation was not successful, then the EEC may perform the required EDGE-1 operations such as create subscriptions at the T-EES.

8.8.2.3 EEC executed ACR via S-EES

In this scenario, the EEC is triggered as a result of the UE's movement as described in 8.8.1.1. Figure 8.8.2.3-1 illustrates the EEC executing ACR via the S-EES.

Pre-condition:

1. The AC at the UE already has a connection to the S-EAS; and
2. The EEC is able to communicate with the S-EES.

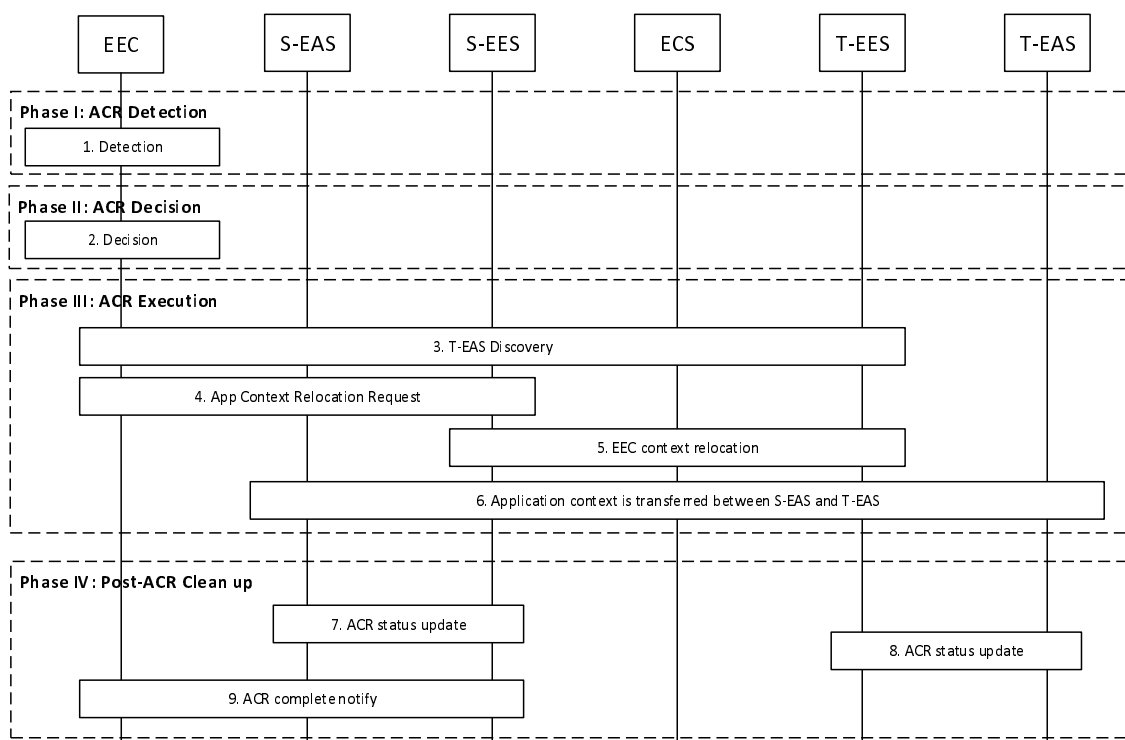


Figure 8.8.2.3-1: EEC executed ACR

Phase I: ACR Detection

1. The EEC detects that ACR may be required as described in clause 8.8.1.1. The EEC may detect that ACR may be required for an expected or predicted UE location in the future as described in clause 8.8.1.1.

Phase II: ACR Decision

2. The EEC decides to proceed required procedures for triggering ACR.

Phase III: ACR Execution

3. The EEC determines the T-EES by using the provisioned information or performing service provisioning procedure per clause 8.3 of the present document. When in step 1 the ACR for service continuity planning is triggered, then the Connectivity information and UE Location in the Service Provisioning (as specified in clause 8.3) procedure contains the expected Connectivity information and expected UE Location. If the UE is

within the service area of the T-EES, upon selecting T-EES the UE may need to establish a new PDU connection to the target EDN. If EEC registration configuration for the T-EES indicates that EEC registration is required, the EEC performs EEC registration with the selected T-EES as specified in clause 8.4.2.2.2. The EEC can then discover and select T-EAS by performing EAS Discovery with the T-EES per clause 8.5.2 of the present document.

NOTE 1: Several EEC registrations with different EESs may result from T-EAS discovery process during a single ACR operation.

4. The EEC performs ACR launching procedure (as described in clause 8.8.3.4) to the S-EES with the ACR action indicating ACR initiation and the corresponding ACR initiation data (with the need to notify the EAS). The S-EES authorises the request from the EEC. The S-EES decides to execute ACR based on the information received from the EEC, EEC context and/or EAS profile. The S-EES may apply the AF traffic influence with the N6 routing information of the T-EAS in the 3GPP Core Network (if applicable) and sends the ACR management notification for the "ACT start" event to the S-EAS, as described in clause 8.6.3, to initiate ACT between the S-EAS and the T-EAS. If the EEC has not subscribed to receive ACR information notifications for ACR complete events from the S-EES, the EEC subscribes for the notifications as described in clause 8.8.3.5.2.
5. If the T-EES is different than the S-EES and the EEC Context at the S-EES is not stale, the S-EES initiates EEC Context Push relocation with the T-EES as described in clause 8.9.2.3. Otherwise, if the T-EES is the same as the S-EES, EEC Context Push relocation is skipped.
6. The S-EAS transfers the application context to the T-EAS at implementation specific time. This process is out of scope of the present specification.

When in step 1 the ACR has been triggered for service continuity planning, if the UE does not move to the predicted location, the EEC does not connect to T-EES, the AC does not connect to the T-EAS. Post-ACR Clean up is skipped.

NOTE 2: The S-EAS or T-EAS can further decide to terminate the ACR, and the T-EAS can discard the application context based on information received from EEL and/or other methods (e.g. monitoring the location of the UE). It is up to the implementation of the S-EAS and T-EAS whether and how to make such a decision.

NOTE 3: When in step 1 the ACR for service continuity planning is triggered, Post-ACR Clean up is performed after the UE moves to the predicted location.

Phase IV: Post-ACR Clean up

7. The S-EAS sends the ACR status update message to the S-EES as specified in clause 8.8.3.8.
8. The T-EAS sends the ACR status update message to the T-EES as specified in clause 8.8.3.8. If the status indicates a successful ACT, and that the EEC Context relocation procedure was attempted but failed, then the T-EES indicates the failure to the T-EAS with the ACR status update response.

NOTE 4: If the EDGE-3 subscription initialization result indicates failure, then the EAS can perform the required EDGE-3 subscriptions at the T-EES.

NOTE 5: Steps 7 and 8 can occur in any order.

9. If the status in step 7 indicates a successful ACT, the S-EES sends the ACR information notification (ACR complete) message to the EEC to confirm that the ACR has completed as specified in clause 8.8.3.5.3. If the EEC Context relocation procedure was attempted, then the notification includes EEC context relocation status IE, indicating the result of the EEC context relocation procedure. If the EEC context relocation status indicates that the EEC context relocation was not successful, then the EEC may perform the required EDGE-1 operations such as create subscriptions at the T-EES.

8.8.2.4 S-EAS decided ACR scenario

In this scenario, the S-EAS may detect the need of ACR locally or is notified by the S-EES via ACR management notifications or UE location notifications. The S-EAS make the decision about whether to perform the ACR, and starts the ACR at a proper time.

Pre-conditions:

1. The S-EAS may depend on the receipt ACR management events from the S-EES, e.g. "user plane path change" events or "ACR monitoring" events as described in clause 8.6.3, to detect the need for an ACR. The S-EAS may also depend on the receipt of UE location notification from the S-EES as described in clause 8.6.2.2.3, to detect the need for an ACR. For the following procedure it is assumed that the S-EAS has subscribed to continuously receive the respective events from the S-EES; and
2. The EEC has subscribed to receive ACR information notifications for target information notification events and ACR complete events from the S-EES, as described in clause 8.8.3.5.2.

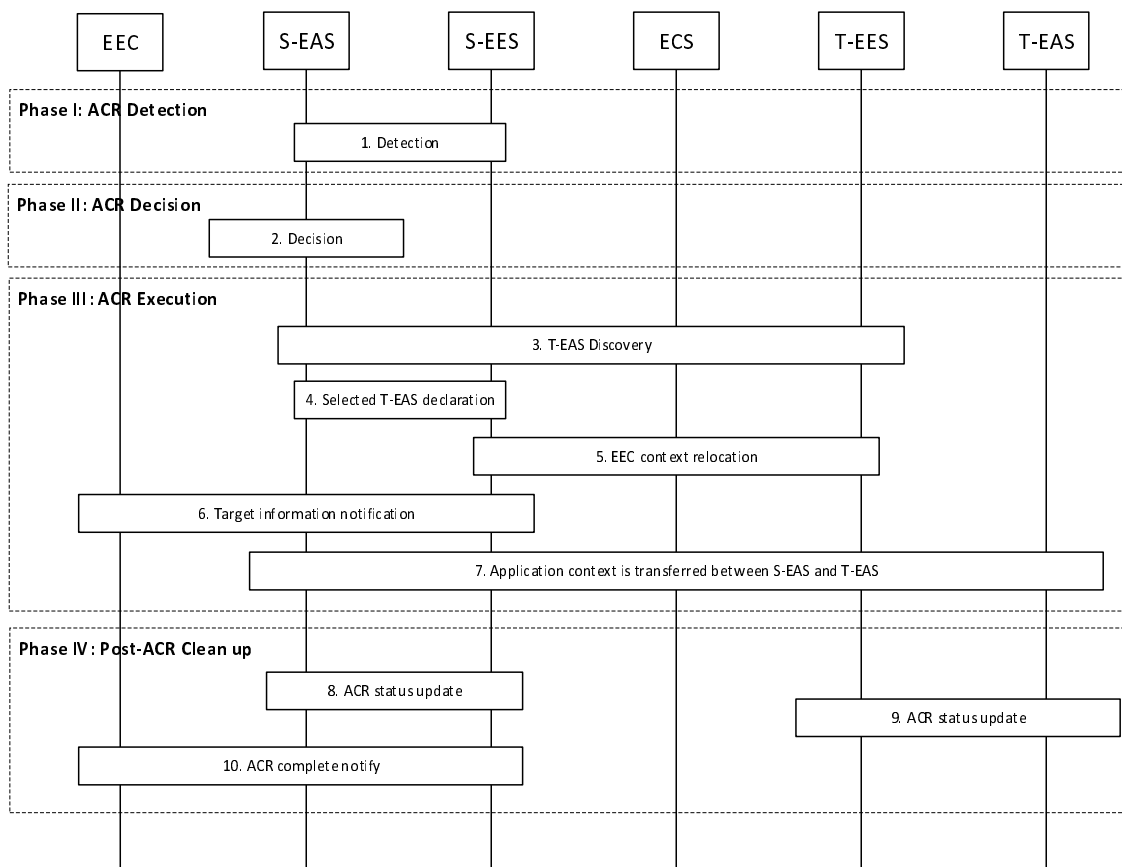


Figure 8.8.2.4-1: S-EAS decided ACR

S-EAS decided ACR is outlined with four main phases: detection, decision, execution and clean up.

Phase I: ACR Detection

1. The S-EAS either receives ACR management notifications from source Edge Enabler Server indicating that ACR may be required ("ACR monitoring" event), or self detects the need for ACR (e.g. upon receipt of a "user plane path change" event or UE location notification). If the ACR management notification indicates "ACR monitoring" event, then the notification will also contain the T-EAS information (see clause 8.6.3.2.3). The S-EAS may detect that ACR may be required for an expected or predicted UE location in the future as described in clause 8.8.1.1.

NOTE 1: How the S-EAS self detects the local need for ACR is outside the scope of this specification.

Phase II: ACR Decision

2. The S-EAS makes the decision to perform the ACR

NOTE 2: How the S-EAS determines when to start the ACR is outside the scope of this specification.

Phase III: ACR Execution

3. The S-EAS discovers the T-EAS as described in clause 8.8.3.2. When in step 1 the ACR has been triggered for service continuity planning, then UE Location and Target DNAI values in the Retrieve T-EES procedure contain the expected UE Location and expected Target DNAI. After S-EAS determines the T-EAS to use, the S-EAS may apply the AF traffic influence with the N6 routing information of the T-EAS in the 3GPP Core Network (if applicable).
4. The S-EAS sends selected T-EAS declaration message to S-EES, to inform S-EES the determined T-EAS to use as described in clause 8.8.3.7.
5. If the T-EES is different than the S-EES and the EEC Context at the S-EES is not stale, the S-EES initiates EEC Context Push relocation with the T-EES as described in clause 8.9.2.3. Otherwise, if the T-EES is the same as the S-EES, EEC Context Push relocation is skipped.
6. Based on the T-EAS selection information received from the S-EAS, the S-EES sends the target information notification to the EEC as described in clause 8.8.3.5.3. The selected T-EES may be included in the target information and the ACID which corresponds to the selected target EAS is included in the notification sent to the EEC as described in clause 8.8.3.5.3.
7. The S-EAS transfers the application context to the T-EAS selected in step 3. This process is out of scope of the present specification.

When in step 1 the ACR has been triggered for service continuity planning, if the UE does not move to the predicted location, the EEC does not connect to T-EES, the AC does not connect to the T-EAS. Post-ACR Clean up is skipped.

NOTE 3: The S-EAS or T-EAS can further decide to terminate the ACR, and the T-EAS can discard the application context based on information received from EEL and/or other methods (e.g. monitoring the location of the UE). It is up to the implementation of the S-EAS and T-EAS whether and how to make such a decision.

NOTE 4: When in step 1 the ACR has been triggered for service continuity planning, Post-ACR Clean up is performed after the UE moves to the expected location.

Phase IV: Post-ACR clean up

8. The S-EAS sends the ACR status update message to the S-EES as specified in clause 8.8.3.8.
9. The T-EAS sends the ACR status update message to the T-EES as specified in clause 8.8.3.8. If the status indicates a successful ACT, and that the EEC Context relocation procedure was attempted but failed, then the T-EES indicates the failure to the T-EAS with the ACR status update response.

NOTE 5: If the EDGE-3 subscription initialization result indicates failure, then the EAS can perform the required EDGE-3 subscriptions at the T-EES.

NOTE 6: Steps 8 and 9 can occur in any order.

10. If the status in step 8 indicates a successful ACT, the S-EES sends the ACR information notification (ACR complete) message to the EEC to confirm that the ACR has completed as specified in clause 8.8.3.5.3. If the EEC Context relocation procedure was attempted, then the notification includes EEC context relocation status IE, indicating the result of the EEC context relocation procedure. If the EEC context relocation status indicates that the EEC context relocation was not successful, then the EEC may perform the required EDGE-1 operations such as create subscriptions at the T-EES.

8.8.2.5 S-EES executed ACR

Figure 8.8.2.5-1 illustrates the S-EES detecting, deciding and executing ACR from the S-EAS to the T-EAS. This may include EELManagedACR by S-EES when initiated by S-EAS as per clause 8.8.3.6.

Pre-condition:

1. The AC at the UE already has a connection to the S-EAS;
2. The EEC is able to communicate with the S-EES;

3. The EEC has subscribed to receive ACR information notifications for target information notification events and ACR complete events from the S-EES, as described in clause 8.8.3.5.2;
4. The S-EAS optionally subscribed to receive ACR management notifications for "ACR facilitation" events to the S-EES, in order to enable detection at S-EAS.
5. In case of EELManagedACR, the T-EAS has subscribed to receive ACT status notifications as described in clause 8.8.3.6.2.3.

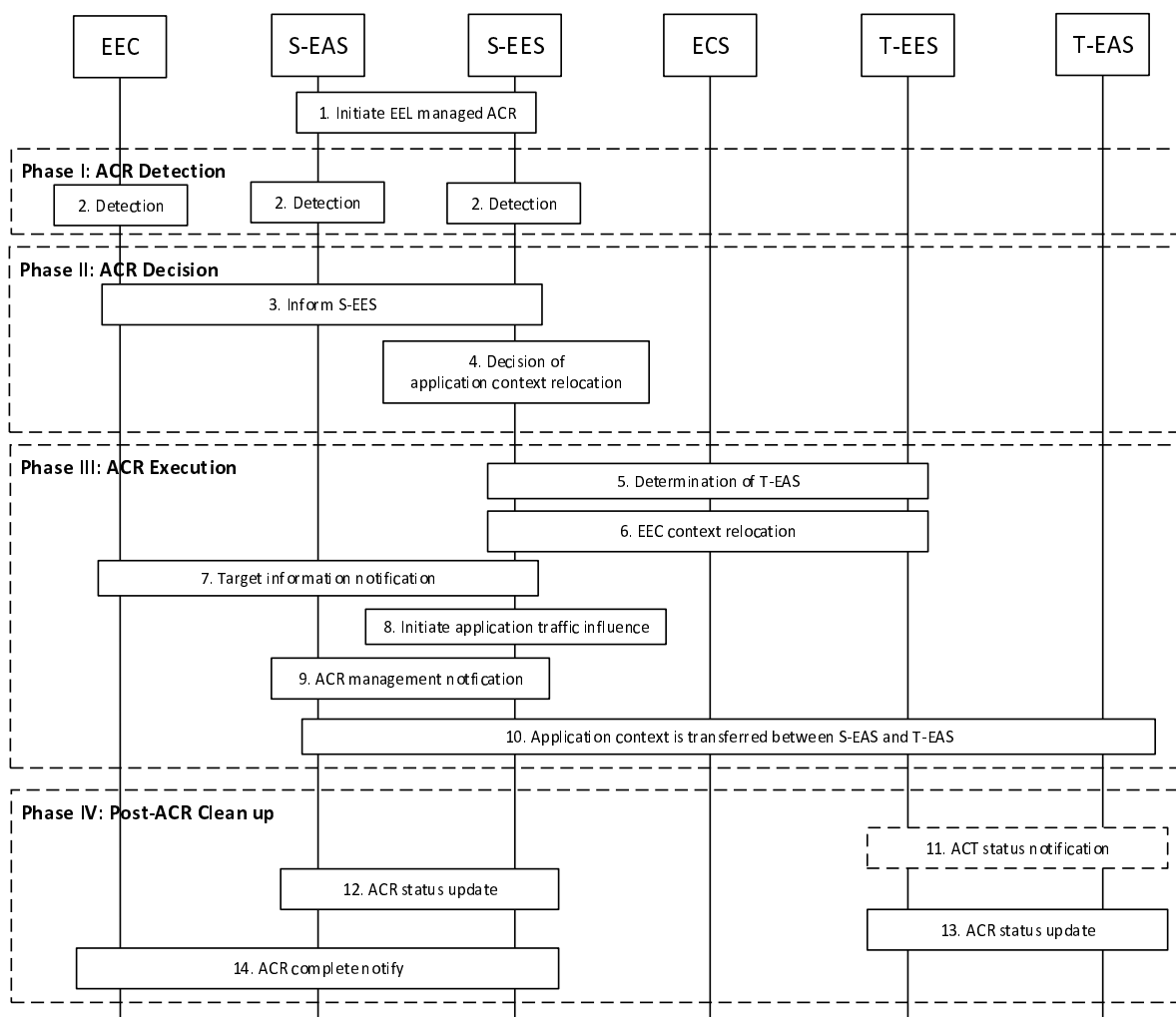


Figure 8.8.2.5-1: S-EES executed ACR

1. The S-EAS may initiate EELManagedACR with S-EES as specified in clause 8.8.3.6. In this step, the S-EAS and S-EES negotiate an address of the Application Context storage to S-EES. The S-EAS puts the Application Context at this address which can be further accessed by the S-EES when the ACT is required.

In this case, the S-EES executes steps 2 (i.e., S-EES detection), 4, 5, 6, 7, 8, 9, 10, 11, 13 and 14. Rest of steps are skipped.

Phase I: ACR Detection

2. Detection entities (S-EAS, S-EES, EEC) detect that ACR may be required as described in clause 8.8.1.1. The detection by the S-EES may be triggered by the User Plane path change notification received from the 3GPP Core Network due to S-EAS request for "ACR facilitation" event (see clause 8.6.3) or due to step 1.

The detection entity may detect that ACR may be required for an expected or predicted UE location in the future as described in clause 8.8.1.1.

Phase II: ACR Decision

3. The detection entity performs ACR launching procedure (as described in clause 8.8.3.4) with the ACR action indicating ACR determination and the corresponding ACR determination data.
4. The S-EES authorises the message if received. The S-EES decides to execute ACR based on the information received or local detection, and the information of EEC context or EAS profile, and then proceed the below steps.

Phase III: ACR Execution

5. The S-EES determines T-EES and T-EAS via the Discover T-EAS procedure in clause 8.8.3.2 of the present document. When in step 2 the ACR has been triggered for service continuity planning, then UE Location and Target DNAI values provided in the Retrieve T-EES procedure contain the expected UE Location and expected Target DNAI. The S-EES may decide not to perform ACR if T-EAS is not available.
6. If the T-EES is different than the S-EES and the EEC Context at the S-EES is not stale, the S-EES initiates EEC Context Push relocation with the T-EES as described in clause 8.9.2.3. Otherwise, if the T-EES is the same as the S-EES, EEC Context Push relocation is skipped.
7. The S-EES sends the target information notification to the EEC as described in clause 8.8.3.5.3.
8. The S-EES may apply the AF traffic influence with the N6 routing information of the T-EAS in the 3GPP Core Network (if applicable).
9. The S-EES sends the ACR management notification (e.g. as notification for "ACR facilitation" event or "ACT start" event as described in clause 8.6.3 or due to step 1) to the S-EAS to initiate ACT between the S-EAS and the T-EAS.
10. The Application Context is transferred from S-EAS to the T-EAS at implementation specific time. In the case of EELManagedACR, the S-EES accesses the Application Context from the address as per step 1 and the S-EES and T-EES engage in the ACT from S-EAS to the T-EAS (obtained as per step 5) in a secure way. Further the T-EAS accesses the Application Context made available by the T-EES. If S-EAS performs the ACT directly with T-EAS, the specification of such process is out of scope of the present document.

NOTE 1: The Application Context is encrypted and protected by the application layer. The S-EES and the T-EES engage in the packet level transport of the Application Context and they have no visibility to the content of the Application Context.

When in step 2 the ACR has been triggered for service continuity planning, if the UE does not move to the predicted location, the EEC does not connect to T-EES, the AC does not connect to the T-EAS. Post-ACR Clean up is skipped.

NOTE 2: The S-EAS or T-EAS can further decide to terminate the ACR, and the T-EAS can discard the application context based on information received from EEL and/or other methods (e.g. monitoring the location of the UE). It is up to the implementation of the S-EAS and T-EAS whether and how to make such a decision.

NOTE 3: When in step 2 the ACR has been triggered for service continuity planning, Post-ACR Clean up is performed after the UE moves to the expected location.

Phase IV: Post-ACR Clean up

11. In case of EELManagedACR, once the ACT is successful, the T-EES sends an ACT status notification to the T-EAS as described in clause 8.8.3.6.2.4, indicating that the Application Context is available.
12. The S-EAS sends the ACT status update message to the S-EES as specified in clause 8.8.3.8.
13. The T-EAS sends the ACR status update message to the T-EES as specified in clause 8.8.3.8. If the status indicates a successful ACT, and that the EEC Context relocation procedure was attempted but failed, then the T-EES indicates the failure to the T-EAS with the ACR status update response.

NOTE 4: If the EDGE-3 subscription initialization result indicates failure, then the EAS can perform the required EDGE-3 subscriptions at the T-EES.

NOTE 5: Steps 12 and 13 can occur in any order.

14. If the status in step 12 indicates a successful ACT, the S-EES sends the ACR information notification (ACR complete) message to the EEC to confirm that the ACR has completed as specified in clause 8.8.3.5.3. If the EEC Context relocation procedure was attempted, then the notification includes EEC context relocation status IE, indicating the result of the EEC context relocation procedure. If the EEC context relocation status indicates that the EEC context relocation was not successful, then the EEC may perform the required EDGE-1 operations such as create subscriptions at the T-EES.

NOTE 6: The Application Client mechanism to support switchover of the application traffic to T-EAS is out of scope of the specification.

8.8.2.6 EEC executed ACR via T-EES

In this scenario, the EEC is triggered as a result of the UE's movement as described in 8.8.1.1. Figure 8.8.2.6-1 illustrates the EEC executing ACR via the T-EES.

Pre-condition:

1. The EEC has the S-EAS information that serves the AC.

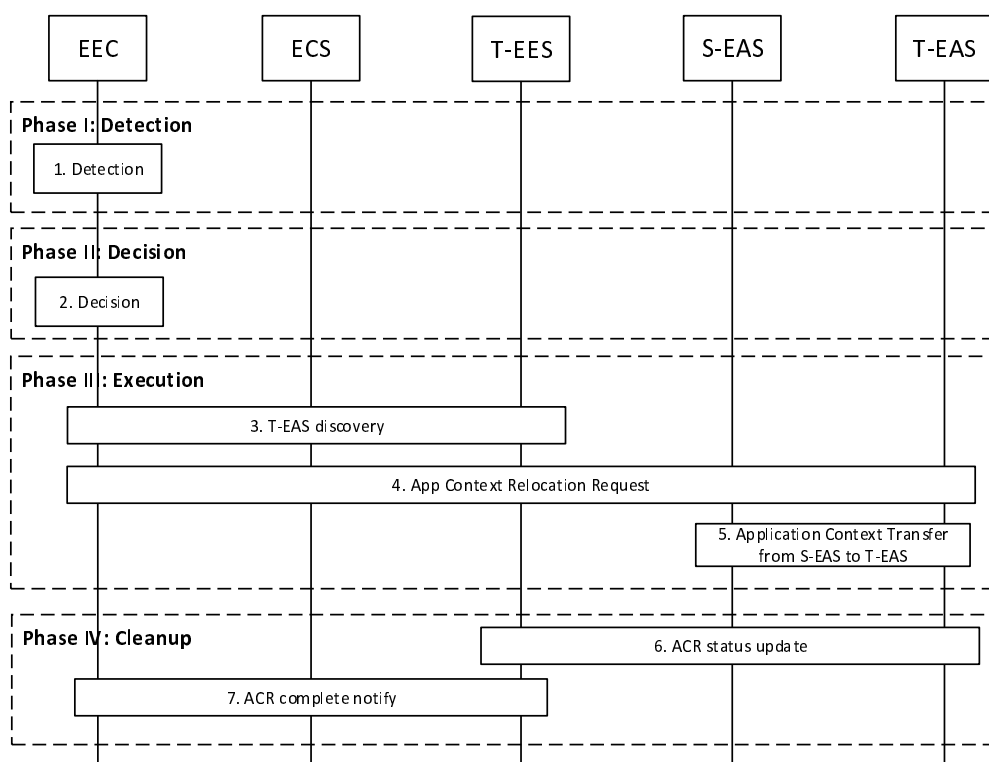


Figure 8.8.2.6-1: EEC executed ACR via T-EES

Phase I: ACR Detection

1. The EEC detects that ACR may be required as described in clause 8.8.1.1. The EEC may detect that ACR may be required for an expected or predicted UE location in the future as described in clause 8.8.1.1.

Phase II: ACR Decision

2. The EEC decides to proceed with required procedures for ACR.

NOTE 1: If supported, the AC can be involved in the decision. It is out of scope of the present document how the AC is involved.

Phase III: ACR Execution

3. The EEC determines the T-EES by using the provisioned information or performing service provisioning procedure per clause 8.3. When in step 1 the ACR for service continuity planning is triggered, then the Connectivity information and UE Location used in the service provisioning procedure contain the expected Connectivity information and expected UE Location. If the UE is within the service area of the T-EES, upon selecting the T-EES the UE may need to establish a new PDU connection to the target EDN. If EEC registration configuration for the T-EES indicates that EEC registration is required, the EEC performs registration with the selected T-EES as specified in clause 8.4.2.2.2. The EEC performs EAS Discovery with the T-EES per clause 8.5.2.

NOTE 2: Several EEC registrations with different EESs may result from T-EAS discovery process during a single ACR operation.

4. The EEC performs ACR launching procedure (as described in clause 8.8.3.4) to the T-EES with the ACR action indicating ACR initiation and the corresponding ACR initiation data (with the need to notify the EAS). If the received ACR initiation request contains an EEC context ID and the S-EES Endpoint, the T-EES performs an EEC Context Pull relocation (clause 8.9.2.2). The T-EES may apply the AF traffic influence with the N6 routing information of the T-EAS in the 3GPP Core Network (if applicable). Then the T-EES sends the ACR management notification with "ACT start" event message to the T-EAS. The EEC also subscribes to receive ACR information notifications for ACR complete events from the T-EES, as described in clause 8.8.3.5.2.
5. The T-EAS initiates ACT between the S-EAS and the T-EAS. This process is out of scope of the present specification.

When in step 1 the ACR has been triggered for service continuity planning, if the UE does not move to the predicted location the EEC does not connect to T-EES, the AC does not connect to the T-EAS. Post-ACR Clean up is skipped.

NOTE 3: The S-EAS or T-EAS can further decide to terminate the ACR, and the T-EAS can discard the application context based on information received from EEL and/or other methods (e.g. monitoring the location of the UE). It is up to the implementation of the S-EAS and T-EAS whether and how to make such a decision.

NOTE 4: When in step 1 the ACR has been triggered for service continuity planning, Post-ACR Clean up is performed after the UE moves to the expected location.

Phase IV: Post-ACR clean up

6. The T-EAS sends the ACR status update message to the T-EES as specified in clause 8.8.3.8. If the status indicates a successful ACT, and that the EEC Context relocation procedure was attempted but failed, then the T-EES indicates the failure to the T-EAS with the ACR status update response.

NOTE5: If the EDGE-3 subscription initialization result indicates failure, then the EAS can perform the required EDGE-3 subscriptions at the T-EES.

7. The T-EES sends the ACR information notification (ACR complete) message to the EEC as described in clause 8.8.3.5.3. If the EEC Context relocation procedure was attempted, then the notification includes EEC context relocation status IE, indicating the result of the EEC context relocation procedure. If the EEC context relocation status indicates that the EEC context relocation was not successful, then the EEC may perform the required EDGE-1 operations such as create subscriptions at the T-EES.

If the procedure fails after step 4, it will be terminated with an appropriate cause in the ACR information notification to the EEC in step 7. The EEC may then proceed attempting to obtain services from the T-EAS discovered in step 3 without service continuity support. Alternatively, the EEC may resume the present procedure starting with step 4 and selecting a different T-EES discovered in step 3 with EAS service continuity support.

NOTE 6: The support of ACR between EDNs operated by different ECSPs is dependent on business agreement between the ECSPs.

8.8.3 Procedures

8.8.3.1 General

8.8.3.2 Discover T-EAS

Figure 8.8.3.2-1 illustrates the procedure for fetching T-EAS information. This procedure may be utilized by a S-EAS, which undertakes the transfer of application context information to a T-EAS directly, or can be invoked by the S-EES itself on deciding to execute ACR.

Pre-conditions:

1. Information related to the EES is available with the S-EAS, if the procedure is triggered by the S-EAS.

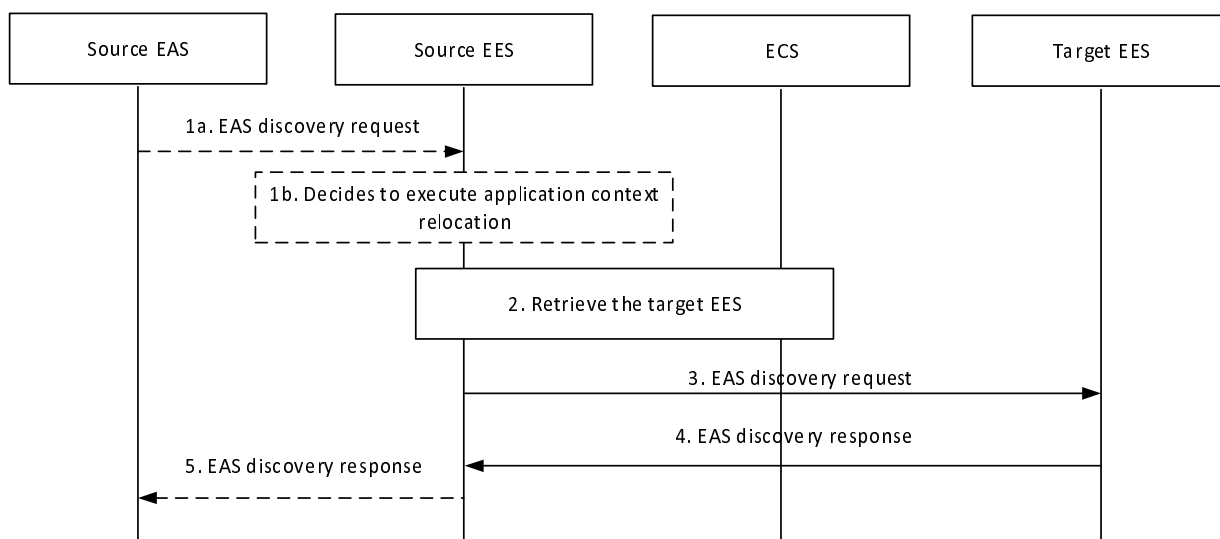


Figure 8.8.3.2-1: Discover T-EAS

1. The S-EAS sends the EAS discovery request to the S-EES or the S-EES decides to execute the ACR. The EAS discovery request from the S-EAS includes the requestor identifier [EASID] along with the security credentials and includes EAS discovery filter matching its EAS profile. If target DNAI is available at the S-EAS via User Plane Path change event, the S-EAS provides the S-EES with the target DNAI. The S-EAS also includes an EAS service continuity support indicator indicating that the S-EAS decided ACR according to clause 8.8.2.4 is to be used for the ACR.

NOTE: The trigger condition to invoke the Discover T-EAS API is up to application service logic, which is out of scope of this specification.

2. If the request is received from the S-EAS, the S-EES checks whether the requesting EAS is authorized to perform the discovery operation. If the UE location is not known to the S-EES or provided by the S-EAS request, then the S-EES may interact with 3GPP core network to retrieve the UE location. If the S-EES decided to execute the ACR or when the requesting EAS is authorized, the S-EES checks if there exists a T-EAS information (registered or cached) that can satisfy the requesting EAS information, additional query filters and the Expected service KPIs and the Minimum required service KPIs if received from the EEC during the EAS discovery or from the S-EAS in step 1. If the S-EES finds the T-EAS(s) in the cached or registered information, the flow either continues with step 5 for the S-EAS triggered discovery or stops for the S-EES decided ACR execution, else the S-EES retrieves the T-EES address from the ECS as specified in clause 8.8.3.3 and continues with step 3.
3. The S-EES invokes the EAS discovery request on the T-EES retrieved from the ECS. The EAS discovery request includes the requestor identifier [EESID] along with the security credentials and includes EAS discovery filter. In the EAS discovery filter, the S-EES may include the Expected service KPIs and the Minimum required service KPIs if received from the EEC during the EAS discovery or from the S-EAS in step 1.

The S-EES also includes the EEC service continuity support indicator received from the EEC during EAS discovery. If in step 1 the S-EES received an EAS service continuity support indicator from the S-EAS, then the S-EES includes this EAS service continuity support indicator and its own EES service continuity support indicator indicating the ACR scenarios supported by the EES. If in step 1 the S-EES decided to execute the ACR, the S-EES includes the EAS service continuity support indicator received from the S-EAS during EAS registration and includes an EES service continuity support indicator indicating that the S-EES executed ACR according to clause 8.8.2.5 is to be used for the ACR.

Upon receiving the request, the T-EES may trigger the EAS management system to instantiate the T-EAS that matches with EAS discovery filter IEs (e.g. ACID) as in clause 8.12.

4. The T-EES discovers the T-EAS(s) and responds with the discovered T-EAS information to the S-EES. To filter T-EAS(s), the T-EES utilizes the discovery filters (e.g. Expected service KPIs and the Minimum required service KPIs) and the indications which ACR scenarios are supported by the AC, the EEC, the S-EES and the S-EAS. The S-EES may cache the T-EAS information.
5. If the request was received from the S-EAS, the S-EES responds to the S-EAS with the discovered T-EAS Information.

8.8.3.3 Retrieve T-EES procedure

Figure 8.8.3.3-1 illustrates the procedure for the S-EES to retrieve the T-EES information from the ECS.

Pre-condition:

1. The S-EES has been pre-configured with the address of the ECS; and
2. The AC at the UE already has on-going application traffic with the S-EAS.

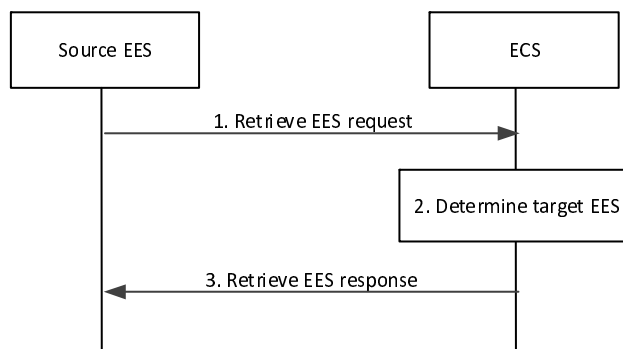


Figure 8.8.3.3-1: Retrieve T-EES procedure

1. The S-EES sends the Retrieve EES request (UE location information or UE identity, EASID of the S-EAS, target DNAI) to the ECS in order to identify the T-EES which has an EAS available to serve the given AC in the UE.
2. If the request contains the UE identity (e.g. GPSI) but the UE location is not known to the ECS, then the ECS interacts with 3GPP core network to retrieve the UE location. The ECS determines T-EES(s) as per the parameters (e.g. EASID, target DNAI) in the request and the UE location information.
3. The ECS sends the Retrieve EES response including the list of EDN configuration information to the S-EES. The list of EDN configuration information includes the EDN details with the endpoint information of T-EES(s) as described in table 8.3.3.3.3-2.

NOTE: The Retrieve EES request initiated by the S-EES can be restricted only to its registered ECS.

8.8.3.4 ACR launching procedure

Figure 8.8.3.4-1 illustrates the ACR launching procedure by the EEC or the S-EAS.

If this procedure is triggered by the EEC, depending on the ACR action indicated in the ACR request, the procedure is used for either ACR initiation or ACR determination. This procedure of the ACR initiation can be re-sent as described in clause 8.8.1.3.

If this procedure is triggered by the S-EAS, the procedure is used for ACR determination.

Pre-condition:

1. The EEC has been authorized to communicate with the EES as specified in clause 8.11, if the procedure is triggered by the EEC; and
2. Information related to the S-EES is available with the S-EAS, if the procedure is triggered by the S-EAS.

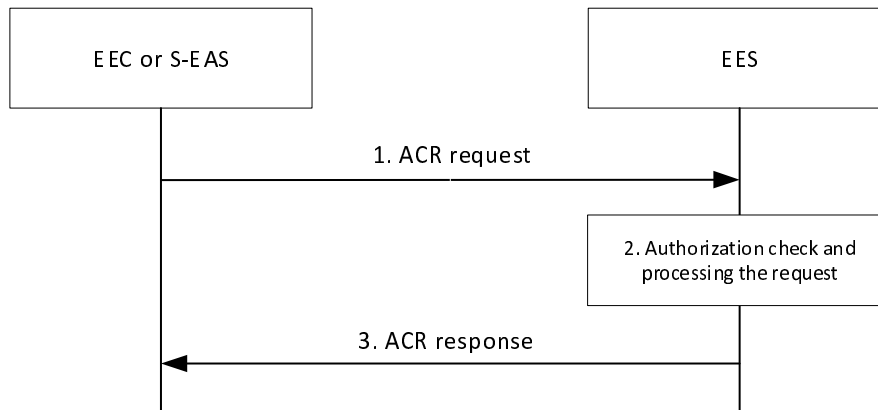


Figure 8.8.3.4-1: ACR launching procedure

1. The EEC or the S-EAS sends an ACR request message to the EES in order to start ACR. The ACR request message includes ACR action to indicate either ACR initiation request or ACR determination request. If the procedure is triggered by the S-EAS, the ACR request message is only for ACR determination.

An ACR request for ACR initiation sent by the EEC:

- includes an indication of whether the EEC requests the EES to perform EAS notification; and
- provides information used by EES to perform AF traffic influence as in 3GPP TS 23 501 [2].

An ACR request for ACR determination sent either by the EEC or the EAS informs the EES that the need for ACR has been detected by the requestor.

2. The EES checks if the requestor is authorized for this operation. If authorized, the EES processes the request and performs the required operations.

If the request in step 1 is for ACR initiation:

- the EES may use information provided in the request to apply the AF traffic influence with the N6 routing information of the T-EAS in the 3GPP Core Network (if applicable), as described in 3GPP TS 23.501 [2], clause 5.6.7.1; and
- if the EAS notification indication in ACR initiation data is provided in the step 1 request and the EAS has subscribed to receive such notification, the EES shall notify the EAS indicated in the ACR initiation data about the need to start ACR by sending an ACR management notification for the "ACT start" event, as described in clause 8.6.3.

If the request in step 1 is for ACR determination, the EES decides to execute ACR as described in clause 8.8.2.5.

If the request in step 1 includes Previous T-EAS Endpoint:

- if the previous EAS notification indication is provided in the step 1 request and the EAS has subscribed to receive such notification, the EES shall notify the EAS about the cancellation of the ACR with the previous T-EAS by sending an ACR management notification for the "ACT stop" event, as described in clause 8.6.3.

- The EAS will inform the remote EAS about application context cancellation, which is outside the scope of this specification. The T-EAS sends the ACR status update message to the T-EES which will include failed result with an appropriate cause **indicating the reason for the failure**.

3. The EES responds to the requestor's request with an ACR response message.

In case of re-sending ACR initiation, if serving EES was changed and EEC context was relocated, the T-EES can clean up any relocated EEC context either indicated in the re-sent ACR request for scenario described in clause 8.8.2.6 or upon reception of the ACR status update with failed result from T-EAS for other scenarios.

8.8.3.5 ACR information subscription

8.8.3.5.1 General

Clause 8.8.3.5.2 and clause 8.8.3.5.3 together illustrate the ACR information procedure based on Subscribe/Notify model.

The ACR information procedure is utilized as a building block for a part of Post-ACR Clean up in clause 8.8.2 and Target information notification.

8.8.3.5.2 Subscribe

Figure 8.8.3.5.2-1 illustrates the ACR information subscription procedure between the EEC and the EES.

Pre-conditions:

1. The EEC has received information (e.g. URI, IP address) related to the EES;
2. The EEC has received appropriate security credentials authorizing it to communicate with the EES as specified in clause 8.11; and
3. The EEC has optionally acquired a Notification Target Address to be used in its subscriptions to notifications.

NOTE: How the EEC acquires the notification target address or a notification channel URI to receive the notifications is out of scope of this release. The notification target address can terminate at the EEC (e.g. in an IoT device) if the deployment supports EEC reachability, or it can terminate at a push notification service. Details of the push notification service are out of scope of this release.

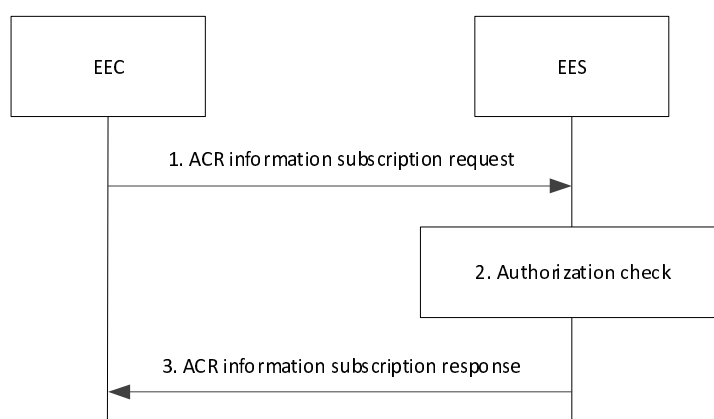


Figure 8.8.3.5.2-1: ACR information subscription

1. The EEC sends an ACR information subscription request to the EES. The request from EEC may include the ACIDs to indicate to the EES which ACs are served by the EEC that need to receive ACR information via EEL.

2. Upon receiving the request from the EEC, the EES checks if the EEC is authorized to subscribe ACR information about the requested EAS(s). If the request is authorized, the EES creates and stores the subscription for ACR information.
3. The EES sends an ACR information subscription response to the EEC, which includes the subscription identifier and may include the expiration time, indicating when the subscription will automatically expire. To maintain the subscription, the EEC shall send an ACR information subscription update request prior to the expiration time. If an ACR information subscription update request is not received prior to the expiration time, the EES shall treat the EEC as implicitly unsubscribed.

8.8.3.5.3 Notify

Figure 8.8.3.5.3-1 illustrates the ACR information notification procedure between the EEC and the EES, which can be used by the EES to notify the EEC of the following:

- target information, i.e. the details of the selected T-EAS and, if required, the selected T-EES, during ACR as described in clauses 8.8.2.4 and 8.8.2.5;

NOTE: The T-EAS and T-EES information can be used to determine the PDU session(s) to provide connectivity to the T-EAS and the T-EES. If the ACR does not require change in EES, i.e. T-EES is same as S-EES, then the T-EES information can be skipped.

- ACR complete events.

Pre-conditions:

1. The EEC has subscribed with the EES for the ACR information as specified in clause 8.8.3.5.2.

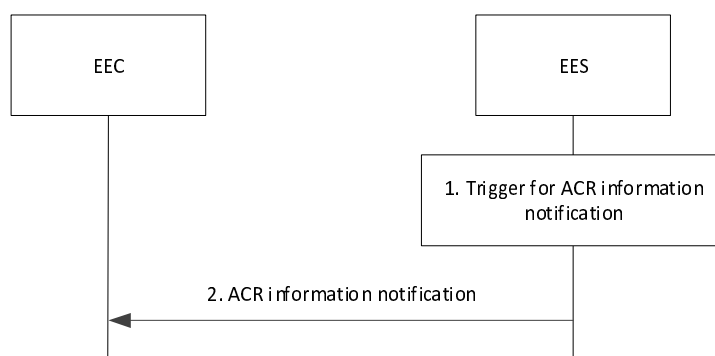


Figure 8.8.3.5.3-1: ACR information notification

1. An event (e.g. ACR complete, or Target information notification) occurs at the EES that satisfies trigger conditions for providing ACR information to a subscribed EEC.
2. The EES sends an ACR information notification to the EEC with the ACR information determined in step 1. The ACR information notification may include ACID to indicate the application context relocation of the AC is complete. If the S-EES has received the successful EEC Context Push response from T-EES, along with registration ID and the registration expiration time in the EEC Context Push relocation procedure, then the ACR information notification towards EEC also includes the registration ID and registration expiration time under EEC context relocation status (for successful status).

8.8.3.5.4 Subscription update

Figure 8.8.3.5.4-1 illustrates the ACR information subscription update procedure between the EEC and the EES.

Pre-conditions:

1. The EEC has subscribed with the EES for the ACR information as specified in clause 8.8.3.5.2.

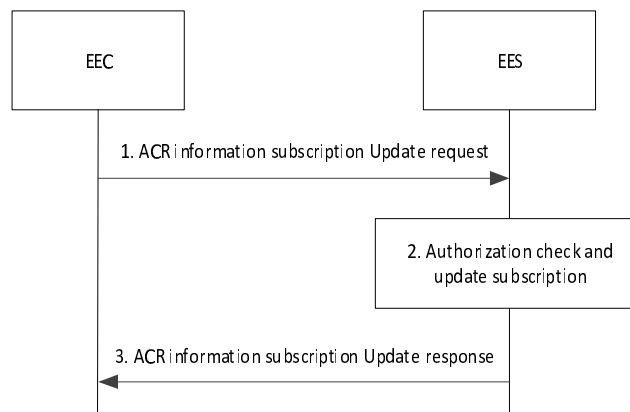


Figure 8.8.3.5.4-1: ACR information subscription update

1. The EEC sends an ACR information subscription update request to the EES.
2. Upon receiving the request from the EEC, the EES checks if the EEC is authorized for the operation. If authorized, the EES updates the subscription.
3. The EES sends an ACR information subscription update response to the EEC.

8.8.3.5.5 Unsubscribe

Figure 8.8.3.5.5-1 illustrates the ACR information unsubscribe procedure between the EEC and the EES.

Pre-conditions:

1. The EEC has subscribed with the EES for the ACR information as specified in clause 8.8.3.5.2.

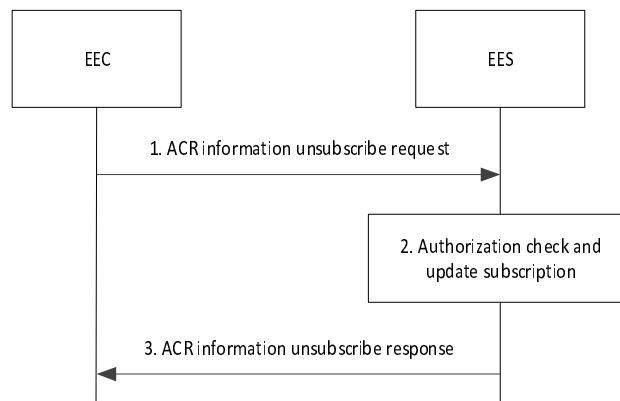


Figure 8.8.3.5.5-1: ACR information unsubscribe

1. The EEC sends an ACR information unsubscribe request to the EES.
2. Upon receiving the request from the EEC, the EES checks if the EEC is authorized for the operation. If authorized, the EES terminates the subscription of the EEC.
3. The EES sends an ACR information unsubscribe response to the EEC.

8.8.3.6 EELManagedACR procedure

8.8.3.6.1 General

This clause introduces a procedure for ACR performed by the Edge Enabler Servers.

When S-EES receives a request for EELManagedACR from S-EAS, the S-EES performs the service operations for the service continuity including detecting the event which may trigger the ACR, making the ACR decision, discovering the T-EAS, accessing and transferring the Application Context to the T-EES/T-EAS, notifying the T-EAS about the available Application Context, notifying the 3GPP network about ACR information, notifying the EEC about the T-EAS information (as per EEC subscription).

The EELManagedACR procedure is designed as an asynchronous operation wherein the S-EES will generate notifications (e.g. failure of any ACR related operation) to the S-EAS while performing the ACR operations.

8.8.3.6.2 Procedure

8.8.3.6.2.1 General

This clause describes the procedures for S-EAS to request for EELManagedACR and for T-EAS to subscribe for ACT status notification.

8.8.3.6.2.2 ACR request

Figure 8.8.3.6.2.2-1 illustrates the procedure for EELManagedACR performed by the Edge Enabler Servers.

Pre-conditions:

1. Information related to the S-EES is available with the S-EAS.
2. The T-EAS has subscribed to the ACR related event from the T-EES.
3. The EEC has subscribed to the ACR related event from the S-EES.

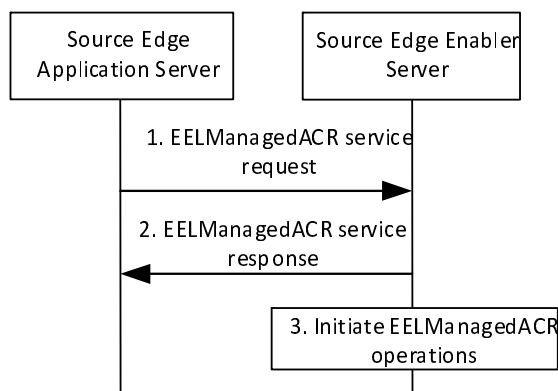


Figure 8.8.3.6.2.2-1: ACR procedure

1. The S-EAS sends an EELManagedACR service request (UE identifier, EAS characteristics for ACR) to request the S-EES to handle all the service operations of the ACR. The S-EAS may initiate this request with S-EES based on different triggers (e.g. when Application Client is connecting to the S-EAS). An address for accessing the Application Context may be provided if available, which allows the S-EES to access the Application Context generated by the S-EAS for ACT.
2. The S-EES checks whether the requesting EAS is authorized to perform the operation. If it is authorized, the S-EES responds with an EELManagedACR service response. If no address for accessing Application Context is provided by S-EAS in step 1, then the S-EES provides an address for storing the Application Context by S-EAS.

NOTE: How the EES accesses the Application Context related to the EAS from the address of the Application Context storage is up to implementation and outside the scope of the present document.

3. The S-EES determines the EELManagedACR operations to be executed as specified in clause 8.8.2.5.

8.8.3.6.2.3 ACT status subscription

Figure 8.8.3.6.2.3-1 illustrates the procedure for T-EAS to subscribe for ACT status during EELManagedACR.

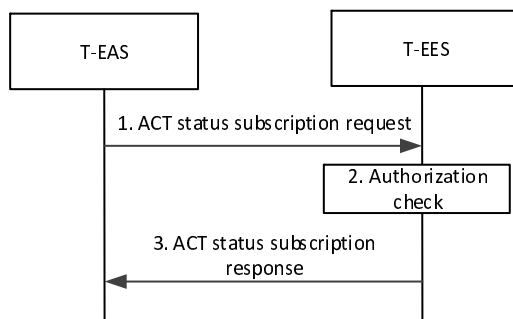


Figure 8.8.3.6.2.3-1: ACR procedure

1. The T-EAS sends an ACT status subscription request to the T-EES.
2. The T-EES checks whether the requesting T-EAS is authorized to perform the operation. If it is authorized, the T-EES creates the subscription.
3. The T-EES responds with the ACT status subscription response

8.8.3.6.2.4 ACT status notification

Figure 8.8.3.6.2.4-1 illustrates the procedure for T-EES to notify the T-EAS about the status of ACT during EELManagedACR.

Pre-conditions:

1. ACT between the S-EES and T-EES has completed.

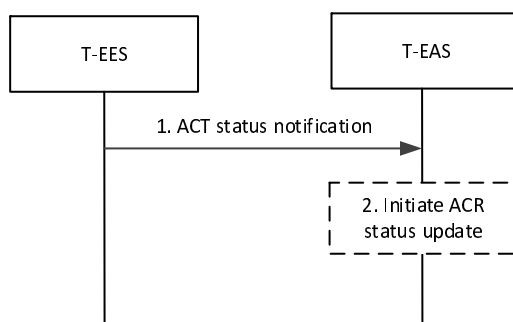


Figure 8.8.3.6.2.4-1: ACR procedure

1. The T-EES sends ACT status notification to the T-EAS, notifying about the status of the ACT between the Application Context received from the S-EES.
2. On receiving a notification about successful ACT, the T-EAS may initiate the ACR status update procedure as described in clause 8.8.3.8.

8.8.3.7 Selected T-EAS declaration

Figure 8.8.3.7-1 illustrates the interactions between the S-EAS and the S-EES for the selected T-EAS declaration.

Pre-conditions:

1. The S-EAS has discovered and selected the T-EAS as described in clause 8.8.3.2.

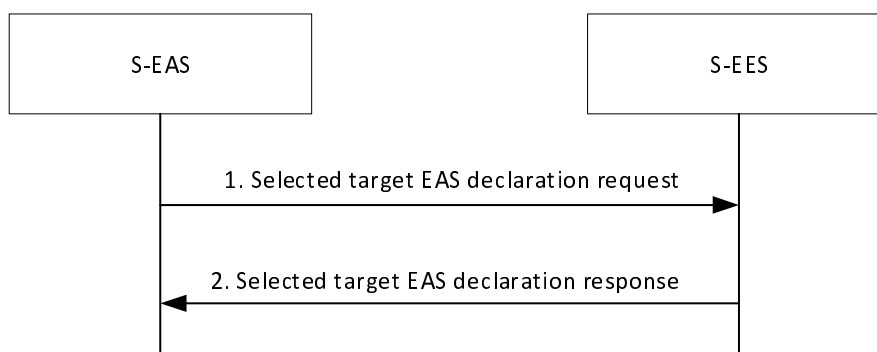


Figure 8.8.3.7-1: Selected target EAS declaration procedure

1. The S-EAS sends Selected target EAS declaration request message to the S-EES. The request includes the information of the selected T-EAS and may include ACID to indicate which AC the T-EAS is intended for.
2. The S-EES checks whether the requesting EAS is authorized to perform operation. If authorized, the S-EES responds to the received request with Selected target EAS notification declaration response message. The S-EES also determines the selected T-EES based on the declared T-EAS selection, then S-EES checks whether the EEC (serving the ACs) has subscribed for ACR related information.

8.8.3.8 ACR status update procedure

Figure 8.8.3.8-1 illustrates the procedure for ACR status update, which is triggered by the S-EAS or the T-EAS. In the post-ACR clean up phase of service continuity scenarios described in clause 8.8.2, this procedure may be used by EAS to indicate the status of ACT to their registrar EESs; or used by the T-EAS to update the notification target address and allow the T-EES to indicate the status of EDGE-3 subscription relocation to the T-EAS including subscription ID update for EDGE-3 subscriptions; or both.

Pre-condition:

1. The ACT procedure between the S-EAS and the T-EAS is either successfully completed or failed.

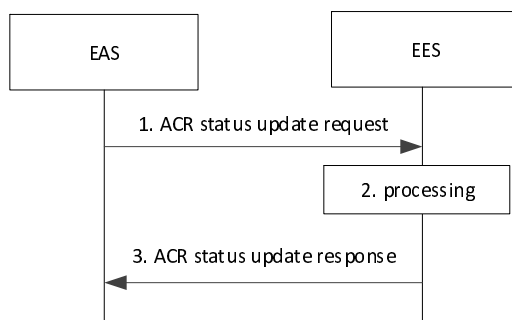


Figure 8.8.3.8-1: ACR status update procedure

1. The EAS sends ACR status update request message to the EES, the request may include the ACT result (success or failure). When sent by the T-EAS, the request may include a list of EDGE-3 subscription ID(s) and Notification Target Address for which the T-EAS wants to update. In case of EELManagedACR, the ACT result is not included by the T-EAS.

2. If the request is authorized by the EES, the EES processes the request. When sent by the T-EAS, if the EDGE-3 subscriptions are available in the T-EES or were successfully relocated during the EEC context relocation procedure, the T-EES updates the Notification Target Address if provided by the T-EAS and may update the list of EDGE-3 subscription ID(s) for the EDGE-3 subscriptions.

When the ACR status update request message of step 1 includes the ACT result, it shall also include the UEID and endpoint information of the other EAS involved in the ACT. The EES uses UEID and EAS endpoint information to identify the corresponding ACR. In cases where the ACT result indicates **failure** of the ACR (i.e. failure with a cause indicating cancellation of the ACR), the T-EES which receives the ACR status update request message removes the transferred EEC context.

3. The EES responds with ACR status update response message to the EAS.

NOTE: If EES is not changed during ACR, the T-EES and S-EES are the same server.

8.8.4 Information flows

8.8.4.1 General

8.8.4.2 EAS discovery request

Table 8.5.3.2-1 describes information elements for the EAS discovery request from the EAS to the EES and from the S-EES to the T-EES. Table 8.5.3.2-2 provides further detail about the EAS Discovery Filter information element.

8.8.4.3 EAS discovery response

The information elements specified in the Table 8.5.3.3-1 is used for the EAS discovery response sent from the EES to the EAS with the following differences:

- The EAS available resources (e.g. memory) indicates the maximum resources available for the AC(s) connected to the S-EAS.

8.8.4.4 ACR request

Table 8.8.4.4-1 describes information elements for the ACR request sent either from the EEC to the S-EES or T-EES, or by the S-EAS to the S-EES.

Table 8.8.4.4-1: ACR request

Information element	Status	Description
Requestor Identifier	M	Unique identifier of the requestor (i.e. EECID or EASID).
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EASID	O	Identifier of the EAS
UE identifier	M	The identifier of the UE (i.e. GPSI).
ACID	O	The identifier of the AC.
ACR action (NOTE 3)	M	Indicates the ACR action (ACR initiation or ACR determination)
ACR initiation data (NOTE 2)	O	ACR initiation IEs to be included in an ACR request message when ACR action indicates it is ACR initiation request.
> T-EAS Endpoint	M	Endpoint information (e.g. URI, FQDN, IP 3-tuple) of the T-EAS.
> Previous T-EAS Endpoint (NOTE 7)	O	Endpoint information (e.g. URI, FQDN, IP 3-tuple) of the T-EAS of the previous ACR.
> DNAI of the T-EAS	O	DNAI information associated with the T-EAS.
> N6 Traffic Routing requirements	O	The N6 traffic routing information and/or routing profile ID corresponding to the T-EAS DNAI.
> EAS notification indication	M	Indicates whether to notify the EAS about the need of ACR.
> Previous EAS notification indication (NOTE 7)	O	Indicates whether to notify the EAS about the cancellation of a previous ACR.
> S-EAS endpoint (NOTE 1)	O	Endpoint information of the S-EAS
> EEC context relocation details	O	Information required for EEC context relocation using the EEC context push or EEC context pull mechanisms.
>> EEC Context ID (NOTE 5)	O	Identifier of the EEC Context
>> S-EES ID (NOTE 5)	O	Identifier of the EES that provided EEC context ID.
>> S-EES endpoint (NOTE 5)	O	The endpoint address (e.g. URI, IP address) of the EES that provided EEC context ID.
>> T-EES ID (NOTE 6)	O	Identifier of the T-EES.
>> T-EES endpoint (NOTE 6)	O	The endpoint address (e.g. URI, IP address) of the T-EES.
ACR determination data (NOTE 2)	O	ACR determination IEs to be included in an ACR request message when ACR action indicates it is ACR determination request.
> S-EAS endpoint	M	Endpoint information of the S-EAS
NOTE 1: This IE shall be present if the EAS notification indication or previous EAS notification indication indicates that the EAS needs to be informed.		
NOTE 2: Either ACR initiation or ACR determination shall be included corresponding to the ACR action.		
NOTE 3: This IE shall indicate ACR determination if the request originates from the S-EAS.		
NOTE 4: Void.		
NOTE 5: This IE may be present only if the request originates from the EEC towards the T-EES.		
NOTE 6: This IE may be present only if the request originates from the EEC towards the S-EES.		
NOTE 7: These IEs shall be present when the EEC re-sends the ACR request as described in clause 8.8.1.3 to indicate a previous ACR is to be cancelled.		

8.8.4.5 ACR response

Table 8.8.4.5-1 describes the information elements for the ACR response sent either from the S-EES to the EEC or S-EAS, or by the T-EES to the EEC.

Table 8.8.4.5-1: ACR response

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

8.8.4.6 Retrieve EES request

Table 8.8.4.6-1 describes the information elements to retrieve T-EES information from the ECS.

Table 8.8.4.6-1: Retrieve EES request

Information element	Status	Description
EESID	M	Unique identifier of the EES.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EASID	M	The EASID.
Target DNAI	O	The target DNAI information which can be associated with potential T-EES(s) and/or T-EAS(s).
UE Identifier	O	The identifier of the UE (i.e. GPSI or identity token)
UE location	O	The location information of the UE. The UE location is described in clause 7.3.2.

8.8.4.7 Retrieve EES response

The information elements specified in the Table 8.3.3.3-1 is used as response for T-EES information retrieval.

8.8.4.8 ACR information subscription request

Table 8.8.4.8-1 describes the information elements for ACR information subscription request from the EEC to the EES.

Table 8.8.4.8-1: ACR information subscription request

Information element	Status	Description
EECID	M	Unique identifier of the EEC.
UE Identifier	O	The identifier of the UE (i.e. GPSI or identity token)
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EASID(s)	M	The identifier of the EAS(s)
ACID(s)	O (NOTE)	The identifier of the AC(s)
Event ID(s)	M	Event ID: - Target information notification - ACR complete
Notification target address	M	Notification target address
Proposed expiration time	O	Proposed expiration time for the subscription
NOTE: If ACID(s) IE is not included, it implies that the subscription corresponds to all ACs that can be served by the EAS(s) included in this message.		

8.8.4.9 ACR information subscription response

Table 8.8.4.9-1 describes the information elements for ACR information subscription response from the EES to the EEC.

Table 8.8.4.9-1: ACR information subscription response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Subscription ID	M	Subscription identifier corresponding to the subscription.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.8.4.10 ACR information notification

Table 8.8.4.10-1 describes the information elements for ACR information notification from the EES to the EEC.

Table 8.8.4.10-1: ACR information notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the EES for the request
EASID	M	The identifier of the EAS
ACID	O	The identifier of the AC corresponding to the Selected target EAS
Event ID	M	Either Target information notification or ACR complete
Target information (NOTE 1)	O	Details of the selected T-EAS and the T-EES.
> T-EAS information	M	Details of the selected T-EAS as described in 'Discovered EAS' IE of Table 8.5.3.3-1.
> T-EES information (NOTE 4)	O	Details of the selected T-EES as described in 'EDN configuration information' IE of Table 8.3.3.3.3-1.
ACR complete event information (NOTE 2)	O	Details of a completed ACR and its result.
Result of ACR (NOTE 2)	M	Indicates whether the ACR is successful or failure
> T-EAS endpoint	M	Endpoint address of the T-EAS to which an ACR has been performed.
EEC Context Relocation status (NOTE 5)	O	Indicates whether the EEC context relocation was successful or not.
> Registration Id (see NOTE 6)	O	Identifier of the registration for the EEC.
> Expiration Time (see NOTE 6)	O	Indicates the expiration time of the registration.
Cause information (see NOTE 3)	O	Indicates the cause information for the failure
NOTE 1: This IE shall be included when Event ID indicates 'Target information notification' event		
NOTE 2: This IE shall be included when Event ID indicates 'ACR complete' event		
NOTE 3: This IE shall be included when the Result of ACR indicates failure.		
NOTE 4: This IE shall be included if the selected T-EES is different from the S-EES. Otherwise, it may be skipped.		
NOTE 5: This IE shall be included when Event ID indicates 'ACR complete' event and EEC context relocation was attempted.		
NOTE 6: This IE shall be included if S-EES has received it in EEC Context Push response.		

8.8.4.11 ACR information subscription update request

Table 8.8.4.11-1 describes the information elements for ACR information subscription update request from the EEC to the EES.

Table 8.8.4.11-1: ACR information subscription update request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be updated
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EASID(s)	O	The identifier of the EAS(s)
Event ID(s)	O	Event ID: - Target information notification - ACR complete
Notification target address	O	Notification target address
Proposed expiration time	O	Proposed expiration time for the subscription

8.8.4.12 ACR information subscription update response

Table 8.8.4.12-1 describes the information elements for ACR information subscription update response from the EES to the EEC.

Table 8.8.4.12-1: ACR information subscription response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.8.4.13 ACR information unsubscribe request

Table 8.8.4.13-1 describes the information elements for ACR information subscription unsubscribe request from the EEC to the EES.

Table 8.8.4.13-1: ACR information unsubscribe request

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription to be updated
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.

8.8.4.14 ACR information unsubscribe response

Table 8.8.4.14-1 describes the information elements for ACR information unsubscribe response from the EES to the EEC.

Table 8.8.4.14-1: ACR information unsubscribe response

Information element	Status	Description
Successful response	O	Indicates that the subscription request was successful.
> Expiration time	O	Indicates the expiration time of the subscription. To maintain an active subscription, a subscription update is required before the expiration time.
Failure response	O	Indicates that the subscription request failed.
> Cause	O	Indicates the cause of subscription request failure

8.8.4.15 EELManagedACR service request

Table 8.8.4.15-1 describes information elements for the EELManagedACR service request from the Edge Application Server to the Edge Enabler Server.

Table 8.8.4.15-1: EELManagedACR service request

Information element	Status	Description
UE identifier	M	Identifies the UE for which ACR is requested
EAS characteristics for ACR	M	Set of characteristics to determine required Edge Application Servers, as detailed in Table 8.5.3.2-2.
Security credentials	M	Security credentials of the source Edge Application Server
Address for Application Context storage	O	The address information from where the Application Context can be accessed for ACT.

8.8.4.16 EELManagedACR service response

Table 8.8.4.16-1 describes information elements for the EELManagedACR service response from the Edge Enabler Server to the Edge Application Server.

Table 8.8.4.16-1: EELManagedACR service response

Information element	Status	Description
Successful response	O	Indicates that the ACR request was successful.
> Address for Application Context storage (NOTE)	O	The address information from where the Application Context can be accessed for ACT.
Failure response	O	Indicates that the EELManagedACR request failed.
> Cause	O	Indicates the cause of request failure
NOTE: This IE is included if "Address for Application Context storage" IE as specified in Table 8.8.4.15-1 is not included in ACR service request.		

8.8.4.17 Selected target EAS declaration request

Table 8.8.4.17-1 describes information elements for the selected target EAS declaration request sent from the S-EAS to the S-EES.

Table 8.8.4.17-1: Selected target EAS declaration request

Information element	Status	Description
UE ID	M	The identifier of the UE.
Security credentials	M	Security credentials.
Selected EAS ID	M	Selected EAS identifier.
ACID	O	The identifier of the AC
Selected EAS Endpoint	M	Endpoint of the selected EAS.

8.8.4.18 Selected target EAS declaration response

Table 8.8.4.18-1 describes information elements for the Selected target EAS declaration response sent from the S-EES to the S-EAS.

Table 8.8.4.18-1: Selected target EAS declaration response

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

8.8.4.19 ACR status update request

Table 8.8.4.19-1 describes the information elements for the ACR status update request from EAS to EES.

Table 8.8.4.19-1: ACR status update request

Information element	Status	Description
EASID	M	The identifier of the EAS providing the update
Security credentials	M	Security credentials of the EAS
ACID	O	The identifier of the AC
ACT result (NOTE 1, NOTE 3)	O	Indicates whether the ACT was successful or failed.
> UEID	M	The identifier of the UE
> EAS endpoint	M	Endpoint address of the other EAS to or from which the ACT has been performed.
List of EDGE-3 subscription ID(s) (NOTE 2, NOTE 3)	O	A list of the EDGE-3 subscription identifiers.
Notification Target Address for EDGE-3 subscription (NOTE 2, NOTE 3)	O	Notification Target Address of the EAS where the notification is to be sent by the EES for EDGE-3 subscription.
NOTE 1: This IE may be included by the S-EAS and T-EAS. In case of EELManagedACR, this IE is not included by the T-EAS.		
NOTE 2: This IE may be included only by the T-EAS.		
NOTE 3: At least one of these IEs shall be present in the message.		

8.8.4.20 ACR status update response

Table 8.8.4.20-1 describes the information elements for the ACR status update response from EES to EAS.

Table 8.8.4.20-1: ACR status update response

Information element	Status	Description
Successful response (NOTE)	O	Indicates that the request was successful.
> EDGE-3 subscription initialization result	O	The IE indicates if the EDGE-3 subscriptions were initialized successfully or if initialization failed.
> List of updated EDGE-3 subscription ID(s)	O	If the EDGE-3 subscription initialization result is successful, the EES provides the updated subscription identifier(s). The absence of an identifier implies no change for the subscription identifier.
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.		

8.8.4.21 ACT status subscription request

Table 8.8.4.21-1 describes the information elements for the ACT status subscription request from EAS to EES.

Table 8.8.4.21-1: ACT status subscription request

Information element	Status	Description
EASID	M	The identifier of the EAS providing the update
Security credentials	M	Security credentials of the EAS
Notification Target Address	M	Notification Target Address of the EAS where the notification is to be sent by the EES

8.8.4.22 ACT status subscription response

Table 8.8.4.22-1 describes the information elements for the ACT status subscription response from EES to EAS.

Table 8.8.4.22-1: ACT status subscription response

Information element	Status	Description
Successful response	O	Indicates that the request was successful.
> Subscription ID	O	Identifier of the subscription
Failure response	O	Indicates that the request failed
> Cause	O	Indicates the cause of request failure

8.8.4.23 ACT status notification

Table 8.8.4.23-1 describes the information elements for an ACT status notification from the EES to the EAS.

Table 8.8.4.23-1: ACT status notification

Information element	Status	Description
Subscription ID	M	Subscription identifier corresponding to the subscription stored in the EES for the request
ACT status	M	Status of the ACT between S-EES and the T-EES

8.8.5 APIs

8.8.5.1 General

Table 8.8.5.1-1 illustrates the APIs for ACR.

Table 8.8.5.1-1: ACR APIs

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_TargetEASDiscovery	Request	Request/Response	EAS, EES
Eees_SelectedTargetEAS	Declare	Request/Response	EAS
Eecs_TargetEESDiscovery	Request	Request/Response	EES
Eees_AppContextRelocation	Request	Request/Response	EEC, EAS
Eees_ACREvents	Subscribe	Subscribe/Notify	EEC
	Notify		
	UpdateSubscription		
	Unsubscribe		
Eees_EELManagedACR	Request	Request/Response	EAS
	Subscribe	Subscribe/Notify	EAS
	Notify		
Eees_ACRStatusUpdate	Request	Request/Response	EAS

8.8.5.2 Eees_TargetEASDiscovery API

8.8.5.2.1 General

This clause describes the Eees_TargetEASDiscovery API and its operations.

8.8.5.2.2 Eees_TargetEASDiscovery_Request operation

API operation name: Eees_TargetEASDiscovery_Request

Description: The consumer requests for the T-EAS information from the EES.

Inputs: See clause 8.8.4.2.

Outputs: See clause 8.8.4.3.

See clause 8.8.3.2 for details of usage of this operation.

8.8.5.3 Eees_AppContextRelocation API

8.8.5.3.1 General

This clause describes the Eees_AppContextRelocation API and its operations.

8.8.5.3.2 Eees_AppContextRelocation_Request operation

API operation name: Eees_AppContextRelocation_Request

Description: The EEC or the EAS requests to start the ACR launching procedure.

Inputs: See clause 8.8.4.4.

Outputs: See clause 8.8.4.5.

See clause 8.8.3.4 for details of usage of this operation.

8.8.5.4 Eecs_TargetEESDiscovery API

8.8.5.4.1 General

This clause describes the Eecs_TargetEESDiscovery API and its operations.

8.8.5.4.2 Eecs_TargetEESDiscovery_Request operation

API operation name: Eecs_TargetEESDiscovery_Request

Description: The consumer requests for the T-EES information from the ECS.

Inputs: See clause 8.8.4.6.

Outputs: See clause 8.8.4.7.

See clause 8.8.3.3 for details of usage of this operation.

8.8.5.5 Eees_ACREvents API

8.8.5.5.1 General

This clause describes the Eees_ACREvents API and its operations.

8.8.5.5.2 Eees_ACREvents_Subscribe operation

API operation name: Eees_ACREvents_Subscribe

Description: The consumer subscribes for ACR related events.

Inputs: See clause 8.8.4.8.

Outputs: See clause 8.8.4.9.

See clause 8.8.3.5.2 for details of usage of this operation.

8.8.5.5.3 Eees_ACREvents_Notify operation

API operation name: Eees_ACREvents_Notify

Description: The consumer is notified about ACR related events.

Inputs: See clause 8.8.4.10.

Outputs: None.

See clause 8.8.3.5.3 for details of usage of this operation.

8.8.5.5.4 Eees_ACREvents_UpdateSubscription operation

API operation name: Eees_ACREvents_UpdateSubscription

Description: The consumer updates an existing subscription for ACR related events.

Inputs: See clause 8.8.4.11.

Outputs: See clause 8.8.4.12.

See clause 8.8.3.5.4 for details of usage of this operation.

8.8.5.5.5 Eees_ACREvents_Unsubscribe operation

API operation name: Eees_ACREvents_Unsubscribe

Description: The consumer unsubscribes for the previously subscribed ACR related events.

Inputs: See clause 8.8.4.13.

Outputs: See clause 8.8.4.14.

See clause 8.8.3.5.5 for details of usage of this operation.

8.8.5.6 Eees_EELManagedACR API

8.8.5.6.1 General

This clause describes the Eees_EELManagedACR API and its operations.

8.8.5.6.2 Eees_EELManagedACR_Request operation

API operation name: Eees_EELManagedACR_Request

Description: The consumer requests for the EELManagedACR handling by the Edge Enabler Server. To use this API, the ASP (EAS provider) and ECSP should have an agreement to use a shared Application Context storage which enables the EES to undertake the ACT in a transparent and secure way, maintaining end user privacy.

Inputs: See clause 8.8.4.15.

Outputs: See clause 8.8.4.16.

See clause 8.8.3.6.2.2 for details of usage of this operation.

8.8.5.6.3 Eees_EELManagedACR_Subscribe operation

API operation name: Eees_EELManagedACR_Subscribe

Description: The consumer requests for the ACT status notifications for EELManagedACR.

Inputs: See clause 8.8.4.21.

Outputs: See clause 8.8.4.22.

See clause 8.8.3.6.2.3 for details of usage of this operation.

8.8.5.6.4 Eees_EELManagedACR_Notify operation

API operation name: Eees_EELManagedACR_Subscribe

Description: The consumer is notified about the ACT status for EELManagedACR.

Inputs: See clause 8.8.4.23.

See clause 8.8.3.6.2.4 for details of usage of this operation.

8.8.5.7 Eees_SelectedTargetEAS API

8.8.5.7.1 General

This clause describes the Eees_SelectedTargetEAS API and its operations.

8.8.5.7.2 Eees_SelectedTargetEAS_Declare operation

API operation name: Eees_SelectedTargetEAS_Declare

Description: The consumer declares the selected T-EAS information to the EES.

Inputs: See clause 8.8.4.17.

Outputs: See clause 8.8.4.18.

See clause 8.8.3.7 for details of usage of this operation.

8.8.5.8 Eees_ACRStatusUpdate API

8.8.5.8.1 General

This clause describes the Eees_ACRStatusUpdate API and its operations.

8.8.5.8.2 Eees_ACRStatusUpdate_Request operation

API operation name: Eees_ACRStatusUpdate_Request

Description: The consumer updates the information related to ACR, e.g. ACT status.

Inputs: See clause 8.8.4.19.

Outputs: See clause 8.8.4.20.

See clause 8.8.3.8 for details of usage of this operation.

8.9 EEC Context and EEC Context relocation

8.9.1 General

EEC Context contains information related to an EEC which is used by EESs to provide the Edge Enabler Layer services. The EEC Context may include information about the EEC-hosting UE and the ACs to which the EEC provides services. The EEC Context information may be collected and maintained at the EES in an EDN while the respective ACs are connected to EASs in that EDN.

EEC Context relocation procedures allow the EEC Context information to be shared between EESs (via EDGE-9 interactions).

The EEC Context information may contain List of EDGE-1 subscriptions (i.e., list of subscription IDs for an EEC). The corresponding EDGE-1 subscription information includes EEC ID, Event ID, subscription ID, 3GPP CN subscription information (optional), notification target address (optional) and filter information (optional).

8.9.1.1 EEC Context handling at EEC registration

An EEC Context shall be created for each registered EEC, after a successful registration, by the receiver EES, as follows:

- If the EEC registration request does not include a previously assigned EEC Context ID value, the receiver EES creates an EEC Context as described in clause 8.2.8. The receiver EES shall assign an EEC context ID and set the source EES Endpoint to its own Endpoint. The EEC ID and UE Identifier shall be set based on the corresponding registration request parameters.
- If the EEC registration request contains an EEC context ID and source EES Endpoint, the receiver (i.e., target) EES performs an EEC Context Pull relocation (clause 8.9.2.2). After a successful EEC Context relocation, the target EES updates the source EES Endpoint with its own Endpoint. The target EES may preserve the EEC Context ID received in the request or assign a new EEC Context ID, subject to EES implementation and local policies.

If the EEC Context relocation is not successful, the target EES creates an EEC Context as described in clause 8.2.8. The target EES shall assign an EEC context ID and set the source EES Endpoint to its own endpoint. The EEC ID and UE ID shall be set based on the corresponding registration request parameters.

After a successful EEC Context Relocation procedure is performed at EEC (re-)registration to a target EES, the source EES shall determine to be stale the EEC Context identified by the EEC Context ID included in the request (i.e., relocated) and the EEC to be de-registered.

8.9.1.2 EEC Context handling at EEC registration update

An EEC Context shall be updated when EEC Registration update requests targeting the corresponding EEC ID are received.

8.9.1.3 EEC Context handling at EEC de-registration

An EEC Context, including the list of Service Session Context(s) information, shall be determined to be stale after a successful EEC de-registration procedure.

NOTE: Stale EEC Context(s) are subject to information persistence policies and privacy policies. Mechanisms for re-use of stale EEC Context(s) are not in scope of the current version of specification.

8.9.1.4 EEC Context handling at Application Context Relocation

The EEC Context provided to a target EES in an EEC Context Pull relocation or an EEC context Push relocation shall be stored at the target EES, as follows:

- If an EEC context with the same EEC ID, EEC Context ID and source Endpoint already exists at the target EES, the EEC Context is updated.
- If an EEC context with the same EEC ID, EEC Context ID and source Endpoint does not exist at the target EES, the EEC Context is stored.

After a successful EEC Context Relocation procedure is performed at ACR, the source EES shall determine to be stale the element(s) of the list of Service Session Context(s) information included in the request (i.e., relocated). If all Service Session Context(s) information in the EEC Context are stale, the EEC Context is determined to be stale and the EEC to be de-registered.

8.9.1.5 Other EEC Context handling

Elements of the list of Service Session Context(s) information shall be created by the EES when it determines that a registered EAS is providing services to an AC on the served EEC.

Editor's Note: How the EES determines that a registered EAS is providing services to an AC is FFS.

Elements of the list of Service Session Context(s) information shall be determined to be stale when the EES determines that a registered EAS is no longer providing services to an AC on the served EEC.

NOTE: In this version of specification, mechanisms used by EES to determine that a registered EAS is no longer providing services to an AC on a served EEC are implementation-dependent.

An EEC Context shall be updated as follows:

- When EEC Context(s) are created, either after a registration request or based on EEC Context relocation procedure, the EES shall check whether the UE Identifier corresponds to an existing EEC Context and update the EEC Context accordingly.
- When EEC subscription requests corresponding to the EEC ID are processed, the "List of EDGE-1 subscriptions" shall be updated accordingly

8.9.2 Procedures

8.9.2.1 General

The following procedures are supported for EEC Context relocation:

- EEC Context Push; and
- EEC Context Pull.

8.9.2.2 EEC Context Pull relocation

An EEC Context is relocated via an EEC Context Pull request initiated by the target EES.

Figure 8.9.2.2-1 illustrates the EEC Context Pull.

Pre-conditions:

1. The source EES has provided the EEC with an EEC Context ID; and
2. The target EES has received the EEC Context ID, source EES Endpoint.

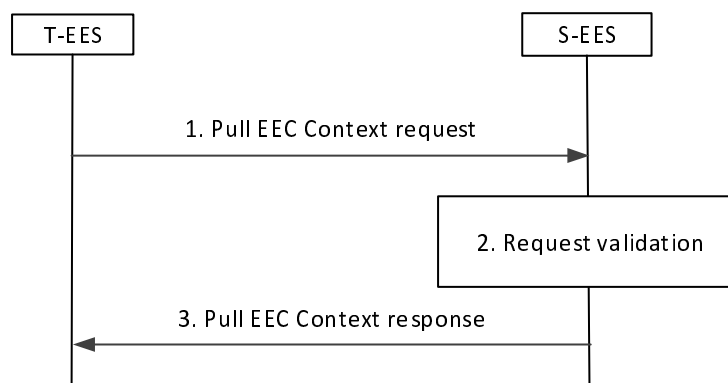


Figure 8.9.2.2-1: EEC Context Pull procedure

1. The target EES requests an EEC Context from the source EES. The request includes EEC Context ID.
2. Upon receiving the request from the target EES, the source EES validates the request and verifies the security credentials of the requester. The source EES uses the EEC Context ID provided to identify and authorize the EEC Context to be relocated.
3. The source EES sends a successful EEC Context response. The target EES stores the received EEC Context.

8.9.2.3 EEC Context Push relocation

An EEC Context is relocated via an EEC Context Push request initiated by the source EES.

Pre-conditions:

1. The source EES has provided the EEC with an EEC Context ID.

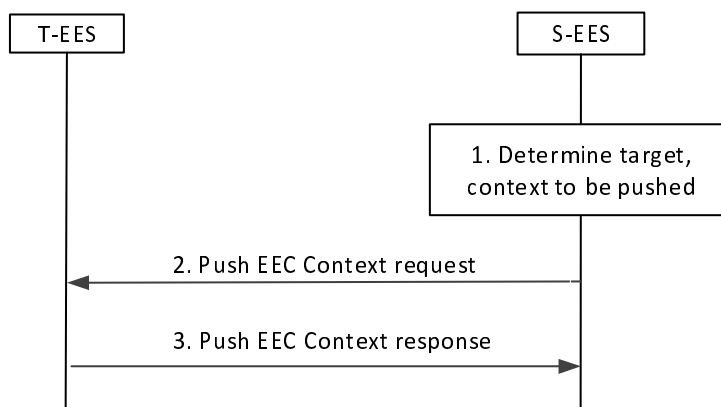


Figure 8.9.2.3-2: EEC Context relocation procedure initiated by source EES

1. The source EES determines to forward EEC Context for relocation to a target EES. The source EES determines the target and the EEC Context to be forwarded.
2. The source EES sends EEC Context Push request to the target EES including the EEC Context determined.
3. Upon receiving the request from the source EES, the target EES validates the request and verifies the security credentials. The target EES uses the EEC Context ID provided to authorize the EEC Context to be stored and managed. Then the target EES sends an EEC Context response indicating success. The T-EES performs implicit registration and creates the registration ID for the registration and includes it in the EEC context push response message for S-EAS decided ACR or S-EES executed ACR scenarios. The S-EES stores the registration details, and when required, notifies the EEC about registration details while sending ACR information notification.

8.9.3 Information flows

8.9.3.1 General

The following information flows are specified for EEC Context relocation:

- EEC Context Pull request and response; and
- EEC Context Push request and response.

8.9.3.2 EEC Context Pull request

Table 8.9.3.2-1 describes information elements in the EEC Context Pull request between two EES.

Table 8.9.3.2-1: EEC Context Pull request

Information element	Status	Description
EES ID	M	Unique identifier of the requesting EES.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EEC Context ID	M	Unique identifier of the EEC Context used to authorize the transfer.
List of Service Session Contexts requested	O	List of Service Session Context IEs requested to be pulled
> EAS ID	M	Identifier of the EAS providing the application services
> EAS Endpoint	M	Endpoint information of the EAS.
> EEC ID	O	Unique identifier of the EEC.

8.9.3.3 EEC Context Pull response

Table 8.9.3.3-1 describes information elements in the EEC Context Pull response between two EESs.

Table 8.9.3.3-1: EEC Context Pull response

Information element	Status	Description
Successful response	O	Indicates that the request was successful.
>EEC Context	O	EEC Context, mandatory if the request was successful
Failure response	O	Indicates that the request failed.
> Cause	O	Indicates the cause of request failure, mandatory if the request failed.

8.9.3.4 EEC Context Push request

Table 8.9.3.4-1 describes information elements in the EEC Context Push request between two EESs.

Table 8.9.3.4-1: EEC Context Push request

Information element	Status	Description
EES ID	M	Unique identifier of the requesting EES.
Security credentials	M	Security credentials resulting from a successful authorization for the edge computing service.
EEC Context	M	EEC Context

8.9.3.5 EEC Context Push response

Table 8.9.3.5-1 describes information elements in the EEC Context Push request between two EES.

Table 8.9.3.5-1: EEC Context Push response

Information element	Status	Description
> registration ID (see NOTE)	O	Identifier of the registration for the EEC
> expiration time (see NOTE)	O	Indicates the expiration time of the EEC registration.
Successful response	O	Indicates that the request was successful.
Failure response	O	Indicates that the request failed.
> Cause	O	Indicates the cause of request failure, mandatory if the request failed.
NOTE: This IE shall be included if implicit registration is performed by T-EES.		

8.9.4 APIs

8.9.4.1 General

Table 8.9.4.1-1 illustrates the EEC context management.

Table 8.9.4.1-1: EEC context management APIs

API Name	API Operations	Operation Semantics	Consumer(s)
Eees_EECContextPull	Request	Request/Response	EES
Eees_EECContextPush	Request	Request/Response	EES

8.9.4.2 Eees_EECContextPull API

8.9.4.2.1 General

This clause describes the Eees_EECContextPull API and its operations.

8.9.4.2.2 Eees_EECContextPull_Request operation

API operation name: Eees_EECContextPull_Request

Description: The consumer requests for the EEC context from the EES.

Inputs: See clause 8.9.3.2.

Outputs: See clause 8.9.3.3.

See clause 8.9.2.2 for details of usage of this operation.

8.9.4.3 Eees_EECContextPush API

8.9.4.3.1 General

This clause describes the Eees_EECContextPush API and its operations.

8.9.4.3.2 Eees_EECContextPush_Request operation

API operation name: Eees_EECContextPush_Request

Description: The consumer pushes the EEC context to another EES.

Inputs: See clause 8.9.3.4.

Outputs: See clause 8.9.3.5.

See clause 8.9.2.3 for details of usage of this operation.

8.10 Utilizing 3GPP core network capabilities

8.10.1 General

The functional entities of the Edge Enabler Layer can utilize the 3GPP core network capabilities (i.e. 5GC, EPC) to fulfill the needs of the edge service operations. This clause specifies the details of the 3GPP core network capabilities consumed by each functional entity.

8.10.2 Capabilities utilized by ECS

When required, the ECS may utilize:

- user plane path management events by subscribing with the 3GPP core network for the user plane path management event notifications of the UE as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3]; and
- the location information from the API exposed by 3GPP core network, e.g. SCEF/NEF/SCEF+NEF or LCS (Location Service) as specified in 3GPP TS 23.682 [17], 3GPP TS 23.502 [3], 3GPP TS 23.271 [7], 3GPP TS 36.305 [8], 3GPP TS 23.273 [9] and 3GPP TS 38.305 [10] to obtain the UE's location from the 3GPP Core Network.

8.10.3 Capabilities utilized by EES

When required, the EES may utilize:

- AF traffic influence functionality, including the user plane path management event notifications of the UE, from the 3GPP core network as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3];
- the location information from the API exposed by 3GPP core network, e.g. SCEF/NEF/SCEF+NEF or LCS (Location Service) as specified in 3GPP TS 23.682 [17], 3GPP TS 23.502 [3], 3GPP TS 23.271 [7], 3GPP TS 36.305 [8], 3GPP TS 23.273 [9] and 3GPP TS 38.305 [10] to obtain the UE's location from the 3GPP Core Network;
- capabilities exposed by the 3GPP core network, e.g. NEF or PCF, to establish an AF session with QoS, and QoS related event notifications subscribed with the 3GPP core network as specified in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.503 [12];
- capabilities exposed by the 3GPP core network, e.g. NEF or NWDAF, to analyse UE expected behaviour as specified in 3GPP TS 23.288 [18]; and
- the monitoring capability exposed by the 3GPP core network as specified in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3].

8.11 EEC Authentication/Authorization

8.11.1 General

The architecture for enabling edge applications supports EEC authentication/authorization.

After the successful EEC authentication/authorization, the EEC acquires a valid security credential for EEC related procedures including service provisioning procedure, EEC registration procedure, EAS discovery procedure and ACR procedure. Detailed procedures are specified in 3GPP TS 33.558 [23].

8.12 Dynamic EAS instantiation triggering

8.12.1 General

The EES may trigger the EAS instantiation dynamically due to e.g., EAS discovery request, UE mobility, upon receiving EEC Registration request containing AC profile.

Upon receiving the EAS discovery request with EAS discovery filter from the EEC or the S-EES during the procedures for EAS discovery or ACR, the EES may fail to discover and select the EAS that matches the UE location and the requesting application characteristics specified in table 8.5.3.2-2 due to no EAS is available or instantiated. The EES may trigger the EAS management system to instantiate the EAS serving the AC in the EDN before returning the EAS information to the EEC or S-EES, based on the pre-configured dynamic EAS instantiation information about which EAS can be dynamically instantiated at the associated EDN.

NOTE 1: The EAS management system is responsible for the authorization of the dynamic EAS instantiation.

NOTE 2: The EAS management system can provide the pre-configured dynamic EAS instantiation information to the EES. Such a mechanism is out of scope of this release of the present document.

NOTE 3: Dynamic EAS instantiation information at the EES is left implementation specific in this version of the specification.

8.13 Charging

The charging procedures are specified in 3GPP TS 32.257 [25].

Annex A (Informative): Deployment models

A.1 General

The following clauses illustrate different aspects of some possible deployment options

- Clause A.2 describes some deployment models for different DN implementations;
- Clause A.3 describes some options for how ECS is deployed in relation to the UE;
- Clause A.4 describes deployment of EES in relation with SEAL services and Application Enabler Services; and
- Clause A.5 describes deployments in relation with CAPIF.

A.2 Deployment models for different DN implementations

A.2.1 General

This clause describes examples of deployment models with respect to different DN implementations as follows:

- option 1. use of non-dedicated DN;
- option 2. use of Edge-dedicated DN; and
- option 3. use of LADN.

The PLMN supporting edge computing services provides connection to one or multiple DNs.

The following clauses describes the detailed deployment models including relationships between EAS service areas, EES service areas, LADN service areas, and PLMN area.

A.2.2 Option 1. Use of non-dedicated DN

There is no Edge-dedicated DN for support of edge computing service. A DN common to other services (e.g. internet access) is used to connect to the EASs.

The PLMN supporting edge computing services provides connection to EASs located in EDNs that respectively corresponds to one or more DNAI(s), and each EDN is identified by DNN and one or more DNAI. UEs establishing PDU sessions for the EASs identify the DN using the same DNN and slice information as for PDU sessions for non-Edge services.

Each EAS and EES can have a topological service area or a geographical service area that the EAS and EES serves, respectively. Within this service area, UEs can access an EAS or an EES regardless of their location within the PLMN area via local breakout.

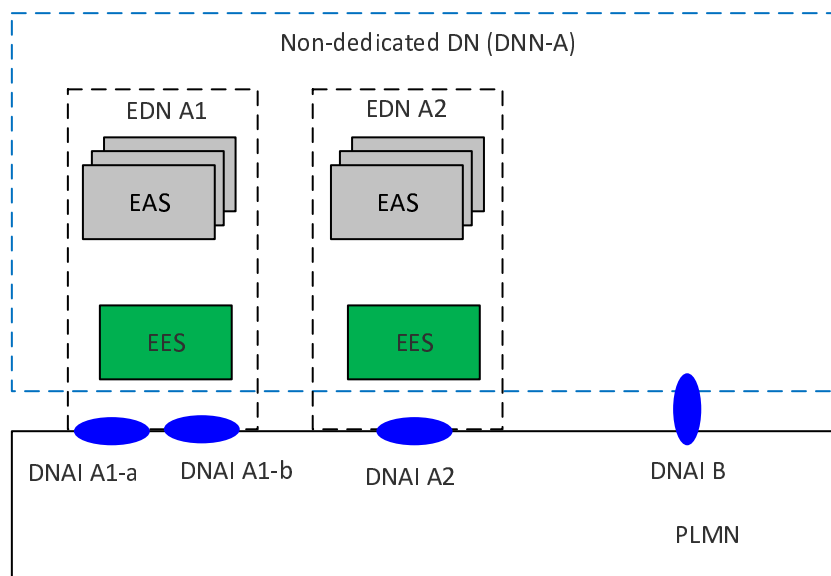


Figure A.2.2-1: Option 1: Use of non-dedicated DN

A.2.3 Option 2. Use of Edge-dedicated DN

The deployment uses Edge-dedicated DNs for support of edge computing service. Each Edge-dedicated DN is configured with unique DNNs.

The PLMN supporting edge computing services provides connection to several EDNs that correspond to one or more DNAI(s), and each EDN is identified by DNN of the Edge-dedicated DN and one or more DNAI.

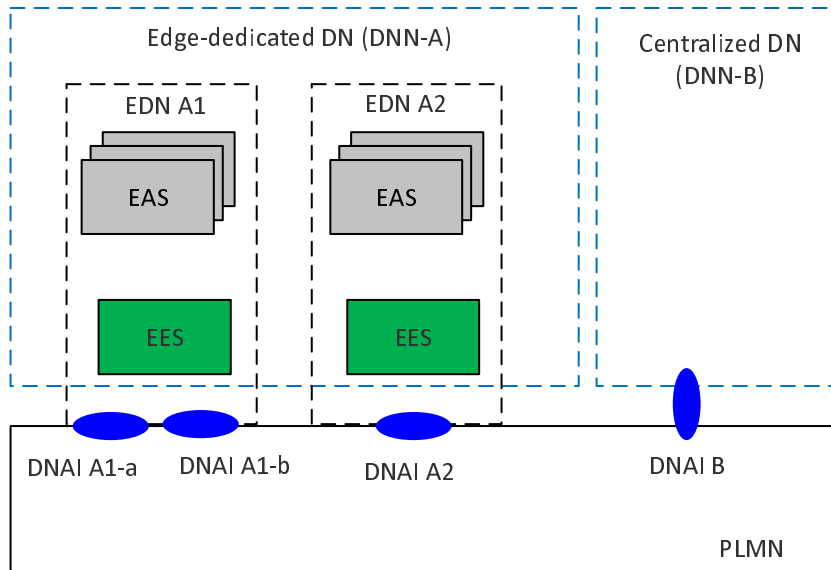


Figure A.2.3-1: Option 2: Use of Edge-dedicated DN

A.2.4 Option 3. Use of LADN

Edge computing services can be provided via Edge-dedicated Data Networks deployed as LADNs. With this option, the PLMN supports edge computing services in the EDN service areas which is equal to the LADN service area. The LADN service area is the service area that the Edge Computing is supported. Each individual EAS in the LADN can support the same or smaller service area than the LADN.

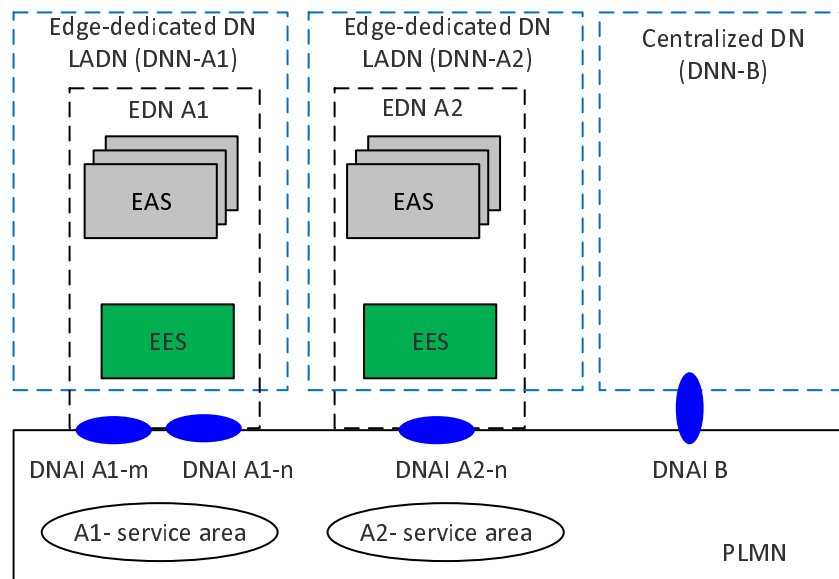


Figure A.2.4-1: Option 3: Use of LADN(s)

A.3 ECS deployments in relation to the UE

A.3.1 General

This clause shows some examples for how the ECS can be deployed in relation to the UE

A.3.2 UE (EEC) served by a single ECS

In this scenario the UE can contain a single AC or multiple ACs, however the UE contains a single EEC which is configured with the address of a single ECS. This could for example be an IoT device that only supports a single AC or a smartphone device which contains many ACs which are served by a single ECS.

A.3.3 UE (EECs) served by multiple ECSs

In this scenario the user is allowed to install multiple ACs in the UE where each AC can be served by an EAS which in turn served by a different ECSP's EES/ECS.

One example is that multiple ACs are installed on a smartphone and the associated EASs are on-boarded onto different ECSP's EESs which are registered with different ECSs.

Another example is a UE that supports Dual SIM. In this scenario the UE can support concurrent connection to two PLMNs.

A.4 Deployment of EES in relation with SEAL services and Application Enabler Services

A.4.1 General

The illustration of layered application architecture with the generic SEAL and Application Enabler server functions available in the cloud is shown in Figure A.4.1-1.

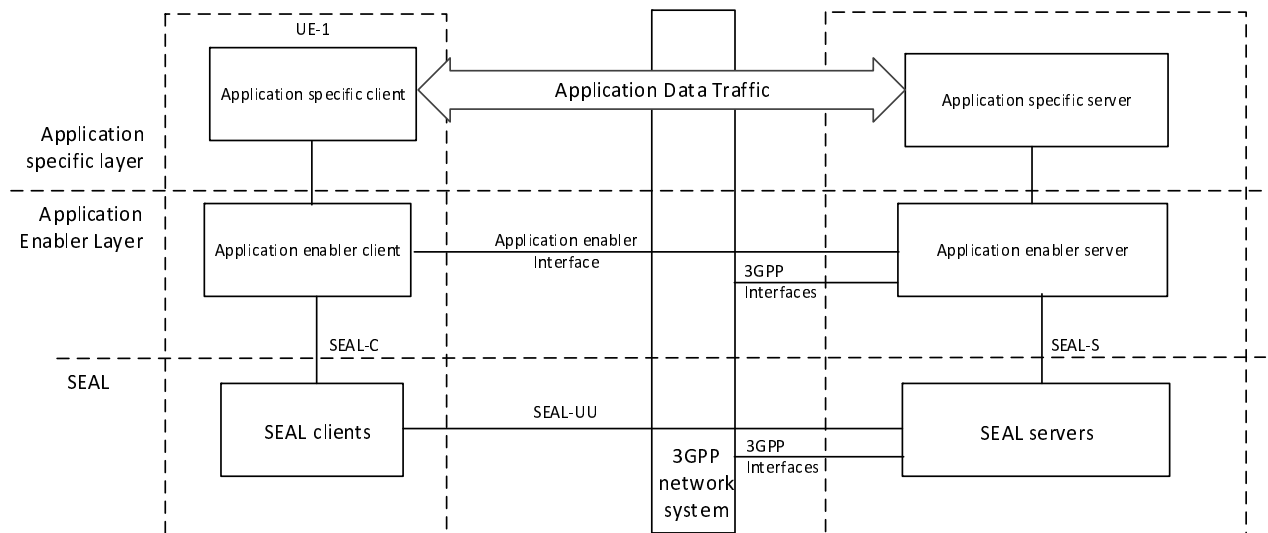


Figure A.4.1-1: Illustration of a layered application architecture with generic SEAL and Application Enabler server functions available in the cloud

The examples of application specific client are V2X application specific client, FF application specific client, UAS application specific client or other vertical application specific client residing on the UE. Similarly, the application specific server could be e.g. V2X application specific server, FF application specific server, UAS application specific server or other vertical application specific server.

The UE may consist of an application enabler client. The examples of application enabler client include V2X application enabler client, FF application enabler client, UAS application enabler client or other vertical application enabler client residing on the UE. Similarly, the application enabler server could be V2X application enabler server, FF application enabler Server, UAS application enabler server or other vertical application enabler server.

The illustration of layered application architecture with generic SEAL and Application Enabler server functions available in the edge is shown in Figure A.4.1-2.

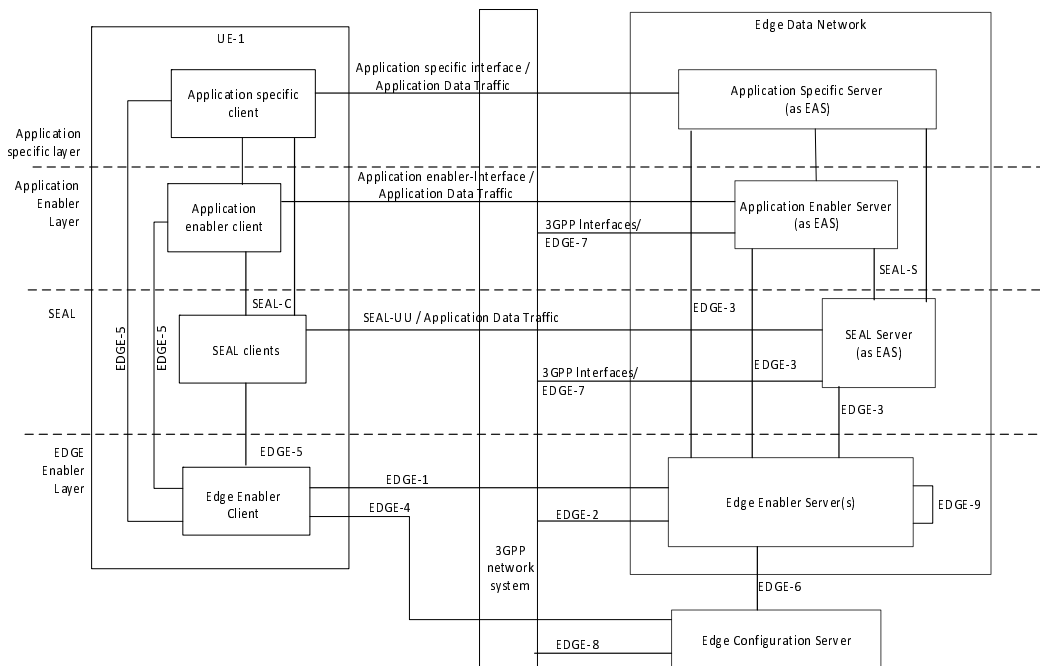


Figure A.4.1-2: Illustration of layered application architecture with generic SEAL and Application Enabler server functions available in the edge

While the server functions of an application specific server can be made available only as an EAS, it is also possible that certain application specific server functions are available both at the edge and in the cloud. Similarly, the server functions of an application enabler server can be made available only as an EAS, it is also possible that certain application enabler server functions are available both at the edge and in the cloud. When the server functions of an application are both available at the edge and the cloud, there may be a need for interaction between the two corresponding application servers, which is out of scope of this specification.

NOTE 1: The details of a specific vertical application architecture based on the generic layered application architecture with server functions of an application available in the edge and the cloud is out of scope of this specification.

NOTE 2: When UE is in the coverage of the EDN due to which certain server functions are available both at the edge and in the cloud, then whether UE connects to the server functions available at the edge or directly to the cloud is out of scope of the present document.

A.4.2 Deployment of SEAL services

There are several options to support SEAL service APIs to be exposed to the EAS.

The EES can act as the CAPIF core function, and the SEAL servers acting the AEF and publish the SEAL service API to the EES. Further, the SEAL service APIs is discovered by the EASs acting as the API invoker during the service API discover procedure as specified in 3GPP TS 23.222 [6].

The EES can act as the API topology hiding entry and re-expose SEAL service APIs as specified in 3GPP TS 23.434 [13] to EAS via EDGE-3 which utilizes the CAPIF-2/2e reference point as specified in 3GPP TS 23.222 [6].

A.4.3 Deployment of Application Enabler services

There are several options to support vertical application enabler server (e.g., V2X application enabler server) APIs to be exposed to the EAS.

The EES can act as the CAPIF core function, and the vertical application enabler server acting the AEF and publish the vertical application enabler server APIs to the EES. Further, the vertical application enabler server APIs is discovered by the EASs acting as the API invoker during the service API discover procedure as specified in 3GPP TS 23.222 [6].

The EES can act as the API topology hiding entry and re-exposes vertical application enabler server APIs, e.g., VAE server APIs as specified in 3GPP TS 23.286 [14] to EAS via EDGE-3 which utilizes the CAPIF-2/2e reference point as specified in 3GPP TS 23.222 [6].

A.5 Deployments in relation with CAPIF

A.5.1 General

A.5.2 Distributed CAPIF

The EES can support EAS's access to northbound APIs exposed by SCEF/NEF by providing distributed CAPIF functions as shown in Figure A.5.2-1.

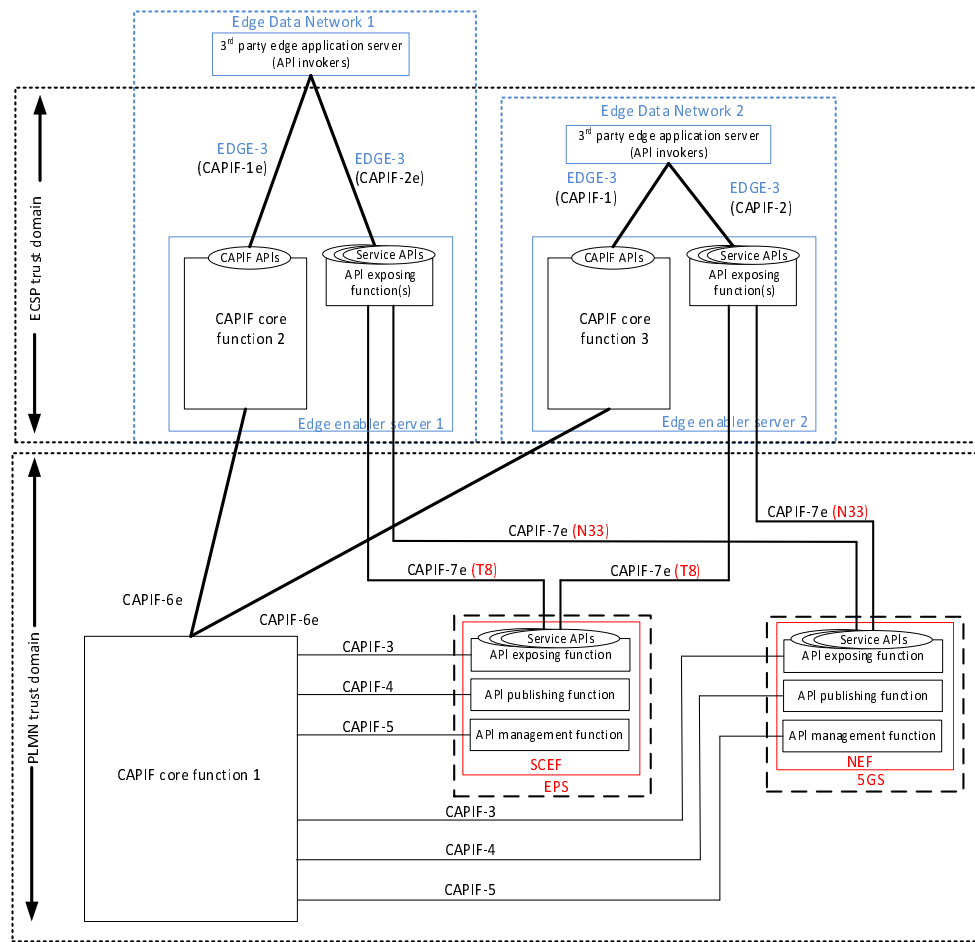


Figure A.5.2-1: EES supporting distributed CAPIF functions

The EDNs reside outside the PLMN trust domain as shown in Figure A.5.2-1. In EDN 2, the EAS and EES are within the same ECSP trust domain. While in EDN 1, the EES and the EAS are in the different ECSP trust domain.

The EES of an EDN provides the following functions for network capability exposure:

- the CAPIF core function as specified in 3GPP TS 23.222 [6] to support onboarding of EASs (API invokers), publish of service APIs, discovery of service APIs and charging of service APIs invocations; and
- the API exposing function as specified in 3GPP TS 23.222 [6] to expose the service APIs from SCEF/NEF to the EASs via proxy or gateway function.

The following procedures are performed as specified in 3GPP TS 23.222 [6]:

- The SCEF and NEF act as API exposing function and the service APIs from SCEF (T8) and NEF (Nnef) are published to the CAPIF core function 1. The service APIs are published to the EESs (CAPIF core function 2 and CAPIF core function 3) from the CAPIF core function 1.
- The EAS acts as an API invoker and is onboarded to the EES (CAPIF core function 2 or CAPIF core function 3) within the EDN.
- The EASs (API invokers) are authenticated with EES (CAPIF core function 2 or CAPIF core function 3).

NOTE: The trusted EASs can utilize the services of a centralized CAPIF core function deployed by the PLMN operator instead of the CAPIF core function of EES deployed within the EDN.

- The EAS discovers the service APIs published by the SCEF and NEF via the EES (CAPIF core function 2 or CAPIF core function 3) within the EDN including the end point address of the API exposing function where the service API invocation is to be performed.

- The EAS obtains authorization to invoke the service APIs of the SCEF and NEF from the EES (CAPIF core function 2 or CAPIF core function 3).
- The EAS invokes the service APIs of the SCEF and NEF after authorization by the EES (API exposing function) and obtaining the UE identifier as specified in clause 8.6.5. The EES (API exposing function) further invokes the service APIs of the SCEF or NEF in the 3GPP core network. EDGE-2 supports CAPIF-7e interactions corresponding to T8 (for SCEF) and N33 (for NEF).

A.5.3 Centralized CAPIF

The EES can support EAS (owned by 3rd party or by PLMN operator) access to northbound APIs exposed by SCEF/NEF by providing centralized CAPIF functions as shown in Figure A.5.3-1.

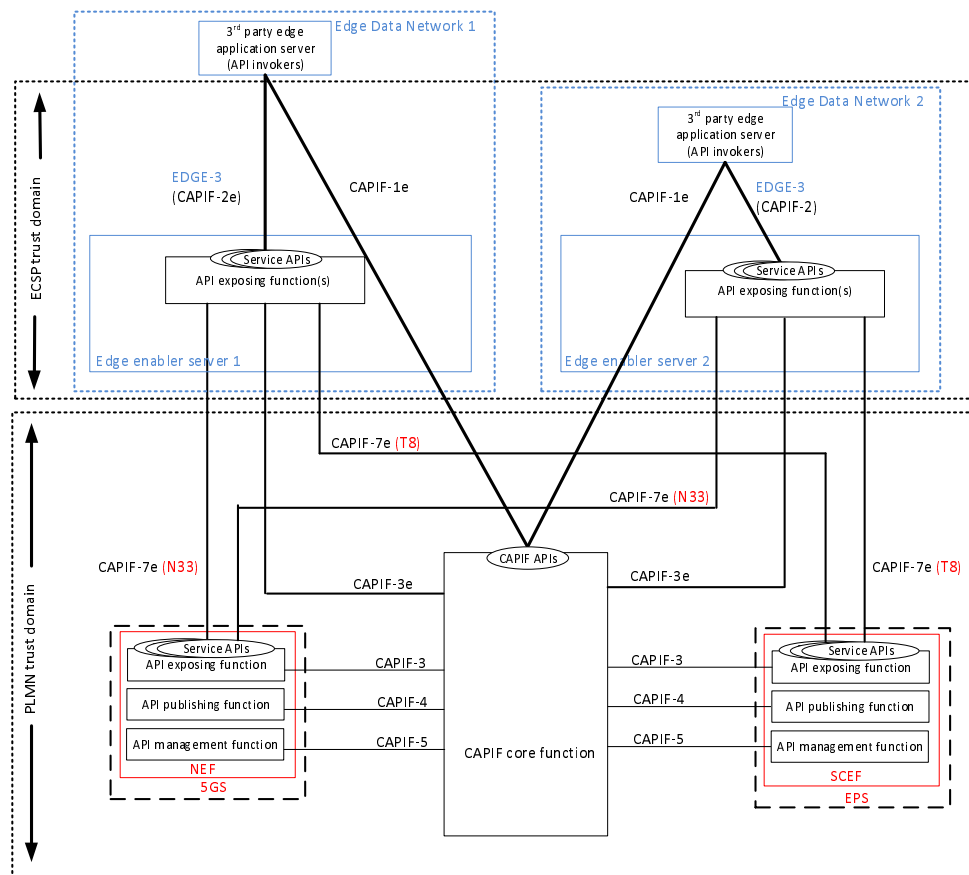


Figure A.5.3-1: EES supporting centralized CAPIF functions

The EDNs reside outside the PLMN trust domain as shown in Figure A.5.3-1. In EDN 2, the EAS and EES are within the same ECSP trust domain. While in EDN 1, the EES and the EAS are in the different ECSP trust domain.

The EES of an EDN provides the following functions for network capability exposure:

- the centralized CAPIF core function as specified in 3GPP TS 23.222 [6] to support onboarding of EASs (API invokers), publish of service APIs, discovery of service APIs and charging of service APIs invocations; and
- the API exposing function as specified in 3GPP TS 23.222 [6] to expose the service APIs from SCEF/NEF to the EASs via proxy or gateway function.

The following procedures are performed as specified in 3GPP TS 23.222 [6]:

- The SCEF and NEF act as API exposing function and the service APIs from SCEF (T8) and NEF (Nnef) are published to the centralized CAPIF core function. The service APIs exposed by the EESs are published to the centralized CAPIF core function.

- The EAS acts as an API invoker and is onboarded to the centralized CAPIF core function residing outside of the EDN.
- The EASs (API invokers) are authenticated with the centralized CAPIF core function.
- The EAS discovers the service APIs published by the SCEF and NEF via the centralized CAPIF core function including the end point address of the API exposing function where the service API invocation is to be performed.
- The EAS obtains authorization to invoke the service APIs of the SCEF and NEF from the centralized CAPIF core function.
- The EAS invokes the service APIs of the SCEF and NEF after authorization by the EES (API exposing function) and obtaining the UE identifier as specified in clause 8.6.5. The EES (API exposing function) further invokes the service APIs of the SCEF or NEF in the 3GPP core network. EDGE-2 supports CAPIF-7e interactions corresponding to T8 (for SCEF) and N33 (for NEF).

Annex B (Informative): Involved entities and relationships

B.1 General

This clause describes the relationship of edge computing service providers, PLMN operators, application service providers and users.

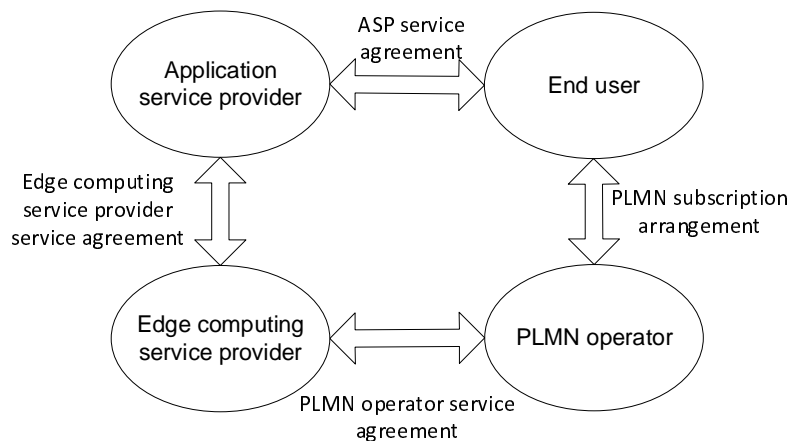


Figure B-1: Relationships involved in edge computing service

The end user is the consumer of the applications provided by the application service provider (ASP) and can have ASP service agreement with a single or multiple application service providers. The end user has a PLMN subscription arrangement with the PLMN operator. The UE used by the end user is allowed to be registered on the PLMN operator network.

The application service provider consumes the edge services (e.g. infrastructure, platform) provided by the edge computing service provider (ECSP) and can have edge computing service provider service agreement with a single or multiple edge computing service providers.

A single PLMN operator can have the PLMN operator service agreement with a single or multiple edge computing service providers.

A single ECSP can have PLMN operator service agreement with a single or multiple PLMN operators which provide edge computing support.

The edge computing service provider and the PLMN operator can be part of the same organization.

Annex C (Informative): Relationship with ETSI MEC architecture

C.1 General

This clause shows an example for how the EDGEAPP architecture and ETSI ISG MEC architecture as specified in ETSI GS MEC 003 [15] can complement each other.

ETSI ISG MEC addresses aspects pertaining to MEC Application enablement through the MEC platform. Additionally, ETSI ISG MEC supports management and orchestration aspects for MEC components.

C.2 Relationship between EDGEAPP and ETSI MEC architectures

Figure C.2-1 provides the relationship of ETSI ISG MEC architecture with EDGEAPP architecture.

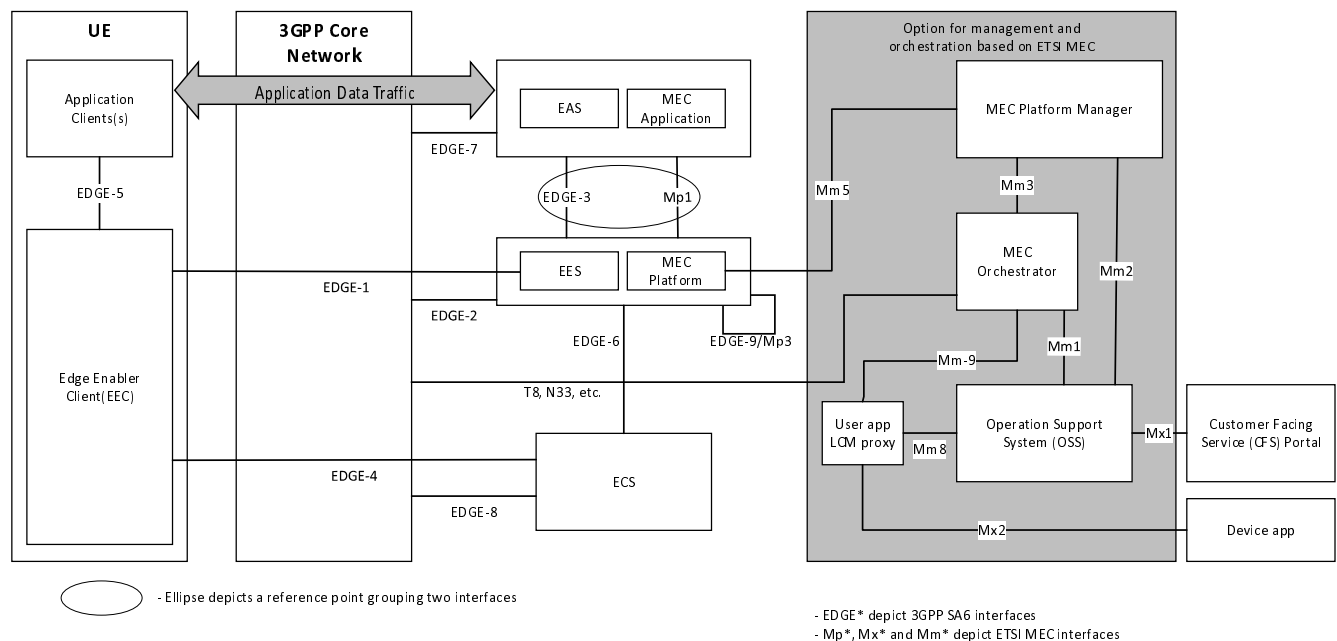


Figure C.2-1: Relationship between EDGEAPP and ETSI MEC architectures

Details about MEC entities (MEC Platform, MEC Application, MEC Platform Manager, MEC Orchestrator, OSS and CFS) can be found in ETSI GS MEC 003 [15].

In ETSI MEC, MEC Applications and MEC Platform can expose services which can include network services, subject to their availability at the core or access network level.

Both EAS and MEC application are application servers and can provide similar application specific functionalities. EAS utilizes the services of EES as specified in this document whereas MEC application utilizes the services provided by MEC platform as specified in ETSI GS MEC 003 [15]. The EAS and MEC application can be aligned in an implementation.

NOTE 1: The details of the functionalities of application servers and alignment are implementation specific.

Both EES and MEC platform provide application support capabilities towards the application servers. How EES and MEC platform are implemented or aligned is implementation specific. Likewise, alignment of the EDGE-3 and Mp1

reference points and EDGE-9 and Mp3 reference points is implementation specific. The EES and MEC platform can be aligned in an implementation.

The orchestration and management aspects of architecture for enabling edge applications are specified in 3GPP TS 28.538 [22].

NOTE 2: The specification of aligned implementation is out of scope in this release.

Annex E (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2020-01	SA6#35	S6-200283				TS skeleton	0.0.0
2020-01	SA6#35					S6-200284, S6-200285, S6-200286, S6-200288, S6-200289, S6-200294, S6-200298, S6-200299, S6-200305, S6-200307, S6-200328, S6-200338, S6-200339, S6-200341, S6-200342, S6-200343, S6-200344, S6-200345, S6-200346, S6-200347, S6-200352, S6-200353, S6-200358	0.1.0
2020-01						Editorial corrections by MCC.	0.1.1
2020-01						Editorial corrections by Rapporteur.	0.1.2
2020-04	SA6#36 BIS-e					S6-200443, S6-200489, S6-200545, S6-200546, S6-200548, S6-200550, S6-200556, S6-200564, S6-200565, S6-200566, S6-200577, S6-200592, S6-200593, S6-200594, S6-200596, S6-200598, S6-200599, S6-200601, S6-200603, S6-200607, S6-200618, S6-200621	0.2.0
2020-06	SA6#37-e					S6-200725, S6-200751, S6-200753, S6-200756, S6-200785, S6-200839, S6-200849, S6-200852, S6-200881, S6-200883, S6-200884, S6-200885, S6-200903, S6-200913, S6-200917, S6-200919, S6-200920, S6-200924, S6-200926, S6-200927, S6-200930, S6-200931, S6-200944, S6-200951, S6-200952, S6-200953, S6-200954, S6-200955	0.3.0
2020-08	SA6#38-e					S6-201024, S6-201028, S6-201036, S6-201101, S6-201102, S6-201104, S6-201120, S6-201140, S6-201144, S6-201173, S6-201261, S6-201264, S6-201267, S6-201281, S6-201282, S6-201284, S6-201287, S6-201289, S6-201298, S6-201299, S6-201302, S6-201303, S6-201305, S6-201308, S6-201311, S6-201316, S6-201317, S6-201318, S6-201320, S6-201321, S6-201322, S6-201323, S6-201324, S6-201325	0.4.0
2020-09	SA6#39-e					S6-201448, S6-201450, S6-201457, S6-201584, S6-201591, S6-201592, S6-201605, S6-201607, S6-201608, S6-201609, S6-201610, S6-201611, S6-201612, S6-201613, S6-201614, S6-201622, S6-201623, S6-201626, S6-201627, S6-201635, S6-201636, S6-201674, S6-201675, S6-201676, S6-201677, S6-201678, S6-201679, S6-201680, S6-201681, S6-201682	0.5.0
2020-09	SA#89-e	SP-200828				Presentation for information at SA#89-e	1.0.0
2020-10	SA6#39 BIS-e					S6-201770, S6-201801, S6-201808, S6-201826, S6-201829, S6-201891, S6-201892, S6-201893, S6-201907, S6-201916, S6-201917, S6-201920, S6-201921, S6-201957, S6-201958, S6-201964, S6-201968, S6-201969, S6-201984, S6-201985, S6-202023, S6-202024, S6-202026, S6-202027, S6-202028, S6-202029, S6-202030, S6-202031, S6-202032, S6-202033, S6-202034	1.1.0
2020-11	SA6#40-e					S6-202074, S6-202078, S6-202091, S6-202103, S6-202122, S6-202135, S6-202153, S6-202154, S6-202156, S6-202162, S6-202163, S6-202166, S6-202167, S6-202188, S6-202191, S6-202241, S6-202246, S6-202252, S6-202255, S6-202266, S6-202270, S6-202271, S6-202272, S6-202273, S6-202282, S6-202283, S6-202286, S6-202289, S6-202290, S6-202313, S6-202316, S6-202317, S6-202333, S6-202334, S6-202335, S6-202336, S6-202337, S6-202338, S6-202339, S6-202340, S6-202341, S6-202356, S6-202361	1.2.0
2021-01	SA6#41-e					S6-210042, S6-210116, S6-210118, S6-210131, S6-210139, S6-210201, S6-210206, S6-210207, S6-210222, S6-210227, S6-210229, S6-210230, S6-210231, S6-210232, S6-210238, S6-210241, S6-210243, S6-210277, S6-210285, S6-210289, S6-210290, S6-210291, S6-210306, S6-210309, S6-210334, S6-210335, S6-210336, S6-210337, S6-210338, S6-210339, S6-210340, S6-210341, S6-210342, S6-210343, S6-210344, S6-210345, S6-210346, S6-210347, S6-210348	1.3.0
2021-03	SA6#42-e					S6-210431, S6-210435, S6-210463, S6-210466, S6-210498, S6-210505, S6-210506, S6-210509, S6-210510, S6-210516, S6-210521, S6-210622, S6-210624, S6-210631, S6-210632, S6-210634, S6-210635, S6-210636, S6-210648, S6-210657, S6-210658, S6-210659, S6-210663, S6-210666, S6-210667, S6-210668, S6-210670, S6-210695, S6-210697, S6-210703, S6-210722, S6-210723, S6-210724, S6-210725, S6-210726, S6-210727, S6-210728, S6-210729, S6-210730, S6-210731, S6-210732, S6-210733	1.4.0
2021-03	SA#91-e	SP-210175	0001			Presentation for approval at SA#91-e	2.0.0
2021-04	SA6#42- BIS-e					S6-210802, S6-210872, S6-210882, S6-210884, S6-210955, S6-210956, S6-210980, S6-210982, S6-210983, S6-211002, S6-211005, S6-211013, S6-211018, S6-211022, S6-211052, S6-211054, S6-211055, S6-211056, S6-211079, S6-211108, S6-211109, S6-211110, S6-211111, S6-211113, S6-211114, S6-211115, S6-211116, S6-211117, S6-211119	2.1.0

2021-06	SA#43-e					S6-211174, S6-211176, S6-211177, S6-211206, S6-211235, S6-211267, S6-211274, S6-211328, S6-211345, S6-211356, S6-211373, S6-211375, S6-211376, S6-211383, S6-211384, S6-211419, S6-211421, S6-211423, S6-211424, S6-211436, S6-211437, S6-211471, S6-211472, S6-211473, S6-211474, S6-211475, S6-211476, S6-211477, S6-211478, S6-211479, S6-211488	2.2.0
2021-06	SA#92-e	SP-210472				Presentation for approval at SA#92-e	2.2.1
2021-06	SA#92-e	SP-210580				MCC Editorial update for publication after TSG SA approval (SA#92)	17.0.0
2021-09	SA#93	SP-210961	0001	-	F	Update on ECS configuration information	17.1.0
2021-09	SA#93	SP-210961	0003	2	F	Corrections for AC and EEC initiated ACR scenario	17.1.0
2021-09	SA#93	SP-210961	0004	1	F	Correct service provisioning overview	17.1.0
2021-09	SA#93	SP-210961	0006	2	F	Solve EN for E1 traffic monitoring	17.1.0
2021-09	SA#93	SP-210961	0007		F	Solve EN for scenario#5	17.1.0
2021-09	SA#93	SP-210961	0008	4	F	EEC context relocation	17.1.0
2021-09	SA#93	SP-210961	0009		F	EAS DNAs	17.1.0
2021-09	SA#93	SP-210961	0010		F	Corrections to ACR request and response	17.1.0
2021-09	SA#93	SP-210961	0011	1	F	Reference corrections	17.1.0
2021-09	SA#93	SP-210961	0012		F	Reference updates	17.1.0
2021-09	SA#93	SP-210961	0017	1	F	Adding ACR management event notification	17.1.0
2021-09	SA#93	SP-210961	0019		F	Remove EN on automated ACR service message	17.1.0
2021-09	SA#93	SP-210961	0020		F	Remove the EAS status of EAS discovery filter	17.1.0
2021-09	SA#93	SP-210961	0024	1	F	Resolving EN about Automated ACR terminology	17.1.0
2021-09	SA#93	SP-210961	0026	2	F	Resolving the editor's note on the use of SBA terminology	17.1.0
2021-09	SA#93	SP-210961	0027	4	F	Resolve EN on AC Profile Parameter Ranges IE	17.1.0
2021-09	SA#93	SP-210961	0030	2	F	Corrections to references, descriptions, and clause title of TS 23.558	17.1.0
2021-09	SA#93	SP-210961	0033	1	F	GPSI format	17.1.0
2021-09	SA#93	SP-210961	0034		F	EN on ECS info in UE subscription data	17.1.0
2021-09	SA#93	SP-210961	0036	2	F	ACR preconditions for EEC	17.1.0
2021-09	SA#93	SP-210961	0039	1	F	Corrections to ACR launching procedure	17.1.0
2021-09	SA#93	SP-210961	0040	1	F	Corrections to T-EES discovery	17.1.0
2021-09	SA#93	SP-210961	0041		F	SA3 references	17.1.0
2021-09	SA#93	SP-210961	0044	1	F	Provide EES endpoint in ACR request to enable EEC context relocation during ACR	17.1.0
2021-12	SA#94	SP-211522	0042	5	F	Cancellation Support in ACR	17.2.0
2021-12	SA#94	SP-211522	0053	2	F	Modify the entity description and add abbreviation	17.2.0
2021-12	SA#94	SP-211522	0054	2	F	List of subscriptions to the CN in EEC context	17.2.0
2021-12	SA#94	SP-211522	0056	4	F	Adding DNN/S-NSSAI information in EAS profile	17.2.0
2021-12	SA#94	SP-211522	0057	2	F	Correction on ACR failure alleviation mechanisms	17.2.0
2021-12	SA#94	SP-211522	0058	2	F	Correction on ACR information subscription request	17.2.0
2021-12	SA#94	SP-211522	0060	2	F	Correction on connectivity information	17.2.0
2021-12	SA#94	SP-211522	0062	2	F	Text order and wording corrections for ACR scenarios	17.2.0
2021-12	SA#94	SP-211522	0063	1	F	Edge functional entity relationship to 5G core	17.2.0
2021-12	SA#94	SP-211522	0064	1	F	Correction on EAS description	17.2.0
2021-12	SA#94	SP-211522	0065	1	F	Correct ACR inconsistencies	17.2.0
2021-12	SA#94	SP-211522	0066	1	F	Correct EAS required API	17.2.0
2021-12	SA#94	SP-211522	0069	1	F	Functional entity responsibilities related to ACR	17.2.0
2021-12	SA#94	SP-211522	0072	1	F	Fixes in EAS Discovery procedures	17.2.0
2021-12	SA#94	SP-211522	0074	2	F	Corrections to general requirements for service continuity	17.2.0
2022-03	SA#95	SP-220103	0079	1	F	Fix consistency issue	17.3.0
2022-03	SA#95	SP-220103	0081	1	F	Solve ACR API inconsistency	17.3.0
2022-03	SA#95	SP-220103	0085	2	F	Adding missing events for ACR notifications	17.3.0
2022-03	SA#95	SP-220103	0086		F	Correction of ACR request and response messages	17.3.0
2022-03	SA#95	SP-220103	0087	1	F	Unique identification in ACR procedures	17.3.0
2022-03	SA#95	SP-220103	0088	1	F	Unique identification of the EEC context in ACR procedures	17.3.0
2022-06	SA#96	SP-220472	0083	4	F	Implicit registration handling in service continuity	17.4.0
2022-06	SA#96	SP-220472	0089	1	F	Removal of the Editor's Note on dynamic EAS instantiation information	17.4.0
2022-06	SA#96	SP-220472	0090	1	F	Fix S-EAS decided ACR	17.4.0
2022-06	SA#96	SP-220472	0091	1	F	Solve EN in UE ID API	17.4.0
2022-06	SA#96	SP-220472	0092	1	F	Update to EEC registration update procedure	17.4.0
2022-06	SA#96	SP-220472	0093	1	F	Corrections to the ECS configuration information	17.4.0
2022-06	SA#96	SP-220472	0095	3	F	Corrections for selected T-EAS declaration	17.4.0
2022-06	SA#96	SP-220472	0096	1	F	Corrections for incomplete functions of ECS and EDGE-6	17.4.0
2022-06	SA#96	SP-220472	0097	1	F	Corrections to ACT status subscription and notification	17.4.0
2022-06	SA#96	SP-220472	0098	1	F	Issues on usage of ACR with LADNs	17.4.0
2022-06	SA#96	SP-220472	0103	1	F	Solve EN in ACR	17.4.0
2022-06	SA#96	SP-220472	0104	1	F	Solve EN in ACR Correction to the supported functions of EDGE-9	17.4.0
2022-06	SA#96	SP-220472	0106	2	F	Corrections to the incompleteness and format errors	17.4.0

2022-09	SA#97	SP-220919	0108	1	F	Add security info in service provisioning response	17.5.0
2022-09	SA#97	SP-220919	0109	1	F	Clarify location user consent	17.5.0
2022-09	SA#97	SP-220919	0114	1	F	Introduction of a reference to charging	17.5.0
2022-09	SA#97	SP-220919	0117	2	F	Correction to Relationship between EDGEAPP and ETSI MEC architectures	17.5.0
2022-09	SA#97	SP-220919	0122	1	F	Correction of EES discovery to EAS discovery	17.5.0
2022-12	SA#98	SP-221238	0143		F	Correction of ACR management notification	17.6.0

History

Document history		
V17.3.0	May 2022	Publication
V17.4.0	July 2022	Publication
V17.5.0	October 2022	Publication
V17.6.0	January 2023	Publication