ETSI TS 123 256 V17.7.0 (2024-01)

5G;
Support of Uncrewed Aerial Systems (UAS) connectivity, identification and tracking;
Stage 2
(3GPP TS 23.256 version 17.7.0 Release 17)

Reference
RTS/TSGS-0223256vh70

Keywords
5G

ETSI

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

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

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

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Legal Notice

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

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

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

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

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

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

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

can indicates that something is possible

cannot indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

1 Scope

The present document specifies architecture enhancements for supporting Uncrewed Aerial Systems (UAS) connectivity, identification, and tracking, according to the use cases and service requirements defined in TS 22.125 [5].

The following functions are specified:

- UAV Identification, authentication and authorization.
- UAV tracking in the 3GPP system:
  - this includes how the 3GPP system can provide support for UAV to ground identification (e.g. to authorized third parties such as police devices).
- handling of unauthorized UAVs and revocation of authorization.

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)".

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

[4] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs".

[5] 3GPP TS 22.125: "Unmanned Aerial System (UAS) support in 3GPP".

[6] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[7] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[8] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[9] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[10] 3GPP TS 33.256: "Security aspects of Uncrewed Aerial Systems (UAS)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 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 TR 21.905 [1] or TS 23.501 [2].

3GPP UAV ID: Identifier assigned by the 3GPP system and used by external AF (e.g. USS) to identify the UAV. GPSI is used as the 3GPP UAV ID.

Broadcast Remote ID: The capability of providing Remote Identification and Tracking over broadcast radio links.

NOTE 1: In the scope of this release, the radio link for Broadcast Remote ID is assumed to utilize radio technologies outside the scope of 3GPP.

CAA (Civil Aviation Administration)-Level UAV Identity: a UAV identity assigned by USS/UTM, and uniquely identifies a UAV at least within the scope of a USS.

Command and Control (C2) Communication: the user plane link to deliver messages with information of command and control for UAV operation from a UAV controller or a UTM to a UAV or to report telemetry data from a UAV to its UAV controller or a UTM.

C2 Aviation Payload: Contains application layer information sent by the UAS to the USS containing UAV pairing information and/or flight authorization information that is transparent to the 3GPP System.

C2 Authorization Payload: Contains application layer information sent by the USS to the UAV containing e.g. C2 pairing information and/or C2 security information that is transparent to the 3GPP System.

C2 Pairing Information: Contains UAV-C Addressing Information which may e.g. include the UAV-C IP Address.

Networked UAV Controller: a UAV Controller connected to the 3GPP network and connected to the UAV via a 3GPP network.

Non-Networked UAV Controller: a UAV Controller not connected to the 3GPP network and connected to UAV via a transport outside the scope of 3GPP, e.g. internet connectivity or direct wireless communication over a technology outside the scope of 3GPP.

Networked Remote ID: The capability of providing Remote Identification and Tracking to a USS over 3GPP network.

Remote Identification (Remote ID) of UAS: The ability of a UAS in flight to provide identification and tracking information that can be received by other parties, to facilitate advanced operations for the UAS (such as Beyond Visual Line of Sight operations as well as operations over people), assist regulatory agencies, air traffic management agencies, law enforcement, and security agencies when a UAS appears to be flying in an unsafe manner or where the UAS is not allowed to fly. The Remote ID information payload may include Serial Number or Session ID assigned to the UAV, location of the ground-station controller, emergency status indication, etc.

Third Party Authorized Entity: is either a privileged Networked UAV Controller, or a privileged Non-Networked UAV Controller, or another entity which gets information on sets of UAV controllers and UAVs from the 3GPP network, and may be connected to the UAV via the Internet; it may be authorized by the UTM to interface with sets of UAV(s).

UAS NF: a 3GPP UAS Network Function for support of aerial functionality related to UAV identification, authentication/authorization and tracking, and to support Remote Identification.

UAS Service Supplier (USS): An entity that provides services to support the safe and efficient use of airspace by providing services to the operator / pilot of a UAS in meeting UTM operational requirements. A USS can provide any subset of functionality to meet the provider's business objectives (e.g. UTM, Remote Identification). In the scope of this specification, the term USS refers to both USS and USS/UTM.

UAS Traffic Management (UTM): a system that can safely and efficiently integrate the flying UAV along with other airspace users. It provides a set of functions and services for managing a range of autonomous vehicle operations (e.g. authenticating UAV, authorizing UAS services, managing UAS policies, and controlling UAV traffics in the airspace).

UAV controller: The UAV controller of a UAS enables a drone pilot to control an UAV.

UAV operator: the entity owning and operating a UAV.

UAS Container: A container to the 3GPP system that includes UUAA Aviation/Authorization Payload and/or C2 Aviation/Authorization Payload. The internal content of the individual payloads is transparent to the 3GPP system.

UAS Services: refers to establishment of connectivity for a UAS for communication with USS, for C2, for remote identification, and for UAV location and tracking.

USS communication: A communication between a UAV and a USS other than C2 communication, by means of user plane data transmission for some UAS Services.

NOTE 2: The PDU session/PDN connection for C2 communication and the PDU session/PDN connection for USS communication can be common or separate.

UUAA Authorization Payload: Contains application layer information optionally including UUAA result for UAV consumption provided by the USS to the UAS which is transparent to the 3GPP System.

UUAA Aviation Payload: Contains application layer information provided by the UAS to USS and is transparent to the 3GPP System

Uncrewed Aerial System (UAS): Composed of Uncrewed Aerial Vehicle (UAV) and related functionality, including command and control (C2) links between the UAV and the control station, the UAV and the network, and for remote identification. An UAS may comprise of a UAV and a UAV controller.

Unknown UAVs: A list of the UAVs to be identified in the target area and served by the PLMN as the result of the UAV tracking requested by USS/UTM.

UUAA: UAV USS authentication and authorization procedure of the UAV to ensure that the UAV has successfully registered with a USS and has therefore been authorized for operations by the USS. An UAV is authenticated and authorized by USS via a UUAA procedure with the support of the 3GPP system before connectivity for UAS services is enabled.

UUAA-MM: the UUAA procedure optionally performed during registration to a 5GS.

UUAA-SM: the UUAA procedure performed during the establishment of a PDU session and performed during the establishment of a PDN connection.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

BRID	Broadcast Remote Identification
BVLOS	Beyond Visual Line of Sight
C2	Command and Control
NRID	Networked Remote Identification
RID	Remote Identification
TPAE	Third Party Authorized Entity
UAS	Uncrewed Aerial System
UAV	Uncrewed Aerial Vehicle
USS	UAS Service Supplier
UTM	Uncrewed Aerial System Traffic Management
UUAA	USS UAV Authorization/Authentication
UUID	Universal Unique Identifier

4 Architecture model and concepts

4.1 General concept

The architecture enhancements for UAVs introduce the following functionality:

- Authentication and authorization of a UAV with the USS during 5GS registration (optional).
- Authentication and authorization of a UAV with the USS during PDU session establishment and PDN connection establishment.
- Support for USS authorization of C2 Communication.

- A reference model for UAV tracking, supporting three UAV tracking modes: UAV location reporting mode, UAV presence monitoring mode, and list of Aerial UEs in a geographic area. The 3GPP system supports geofencing (for in-flight UAV) and geocaging (for UAV on the ground intending to fly) functionality in USS by providing enablers such as location services, event notification to a subscribing USS, etc.

NOTE: Geofencing/geocaging mechanisms are an air traffic control functionality performed by the USS and are out of scope of this specification. The 3GPP system provides enablers to support geofencing/geocaging functionality in USS, e.g. location services, enablement of C2 connectivity, event notification to a subscribing USS, etc. However, no specific geofencing/geocaging mechanisms are defined in 3GPP.

4.2 Architectural reference model

4.2.1 General

This specification covers UAV functionality provided by 5GC connected to NG-RAN and EPC connected to LTE.

The following functionality is defined for UAV support in the 3GPP system:

- An UAV is authenticated and authorized by USS via a USS UAV Authentication & Authorization (UUAA) with the support of the 3GPP system before connectivity for UAS services is enabled.

- Depending on 3GPP network operator and/or regulatory requirements, the UUAA is performed:

  - In 5GS: either as a separate procedure during the 5GS registration procedure (optional and based on specific PLMN policies, USS requirements, and geographic regulatory requirements), or when the UAV requests user plane resources for UAV operation (i.e. PDU session establishment). The UAV shall support UUAA during Registration and PDU session establishment procedure. The network shall support UUAA during PDU session establishment.

  - In EPS: during the attach procedure and the corresponding PDN connection establishment. The network shall support UUAA during PDN connection establishment. The UAV shall support UUAA during PDN connection establishment procedure.

- A UAV that is provisioned with a CAA-Level UAV ID shall provide the CAA-Level UAV ID in 5GS in both Registration and in PDU Session establishment. In EPC, a UAV that is provisioned with a CAA-Level UAV ID provides the CAA-Level UAV ID in PDN Connection establishment in SM-PCO. The CN determine whether UUAA is executed at 5GS registration or at PDU session/PDN Connection establishment, based on local policies.

- The UUAA is performed at PDU session establishment when the UAV requests user plane resources for UAV operation and the UAV provides its CAA Level ID during PDU session (PDN connection) establishment.

- The UAV flight authorization and UAV-UAVC pairing authorization is performed at PDU session/PDN connection establishment/modification procedures.

- The 3GPP system supports USS authorization of pairing between a UAV and a networked UAVC or a UAVC that connects to the UAV via Internet connectivity during either the establishment of the PDN connection/PDU session for C2 communication or a modification of a PDN connection/PDU session either dedicated to C2 communication or common to USS communication and C2 communication. Modifications of the pairing or re-authorization take place via modification of the established PDN connection/PDU session. During such procedures, the USS provides to the 3GPP system information (e.g. QoS requirement, data flow descriptors, etc.) that enable traffic between the UAV and the UAVC.

NOTE 1: How the USS is made aware of the UAVC is outside the scope of 3GPP in this Release.

- For EPC, the PDN connections used by UAV are served by SMF+PGW-C regardless of whether the UAV support 5G NAS or whether their subscription allows access to 5GC. The APN(s) used by the UAV for contacting USS or for C2 communication always resolves to a SMF+PWG-C.

The following architectural assumptions apply:

- It is assumed that the UAV trying to access UAS services using 3GPP connectivity is already registered with a USS and has been assigned a CAA-Level-UAV ID. The procedure for UAV registration and assignment of

CAA-Level-UAV ID is out of scope of 3GPP. The USS assigns to the UAV a CAA-Level UAV ID, or is made aware of the assigned CAA-Level UAV ID.

- A UAV is associated with an Aerial subscription in the UDM. The Aerial subscription contains aerial UE indication in the Access and Mobility Subscription data (to be used similarly to aerial UE indication defined in EPS), an aerial service indication in the Session Management Subscription data for each DNN dedicated for UAS services (C2 and UUAA-SM) which indicates that corresponding authentication/authorization has to be done using API based mechanism.

- An UAV is identified by USS using a CAA-level UAV ID, and identified by the 3GPP System using a 3GPP UAV ID assigned by the MNO:

  - It is assumed that an aerial subscription associated to a UAV includes at least one GPSI to be used as 3GPP UAV ID.

- A UAV is registered with the USS either before connecting with the 3GPP system or using plain internet connectivity via the 3GPP system. Before registering for UAS services with the 3GPP system, the UAV shall be provisioned with a CAA-Level UAV Identity.

- In roaming scenarios, it is assumed that access to USS is in the VPLMN, thus packet data connectivity for UAV-USS communication is in local breakout, and the UAS NF function is located in the VPLMN.

- In this Release, the UAV uses 3GPP access (i.e. LTE & NR) for 3GPP UAV related operations.

- Activation of RAN aerial features for UAV accessing via E-UTRA reuses the existing mechanism defined in TS 36.300 [7].

NOTE 2: In this Release, an UAV is served by single USS for the duration of the connectivity between the USS and the UAV.

- One or more USS(s) may be present in a specific region and may manage UAVs over one or more 3GPP networks.

- The 3GPP Network subscription for the UAV is not assumed to contain any information about the USS.

- The USS address, if known to the UAV, is configured in the UAV via mechanisms outside the scope of 3GPP.

4.2.2 Logical UAV Reference Architecture

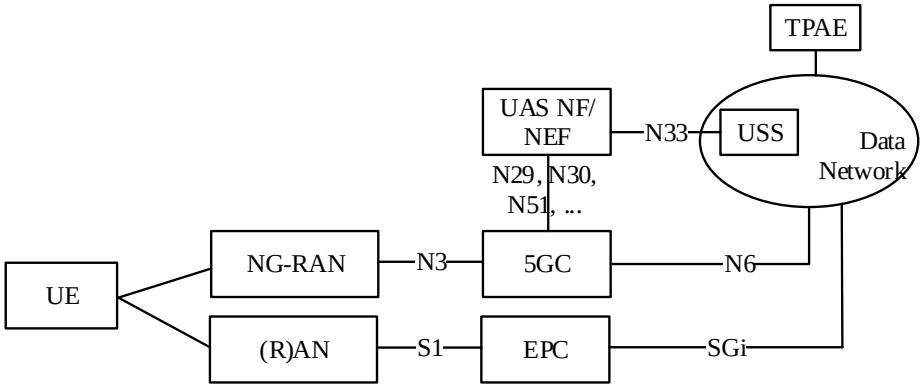

Figure 4.2.2-1: Logical 5GS and EPS architecture for UAV

NOTE 1: Provisioning of UAS services over EPC is based on the use of an SMF+PGW-C node.

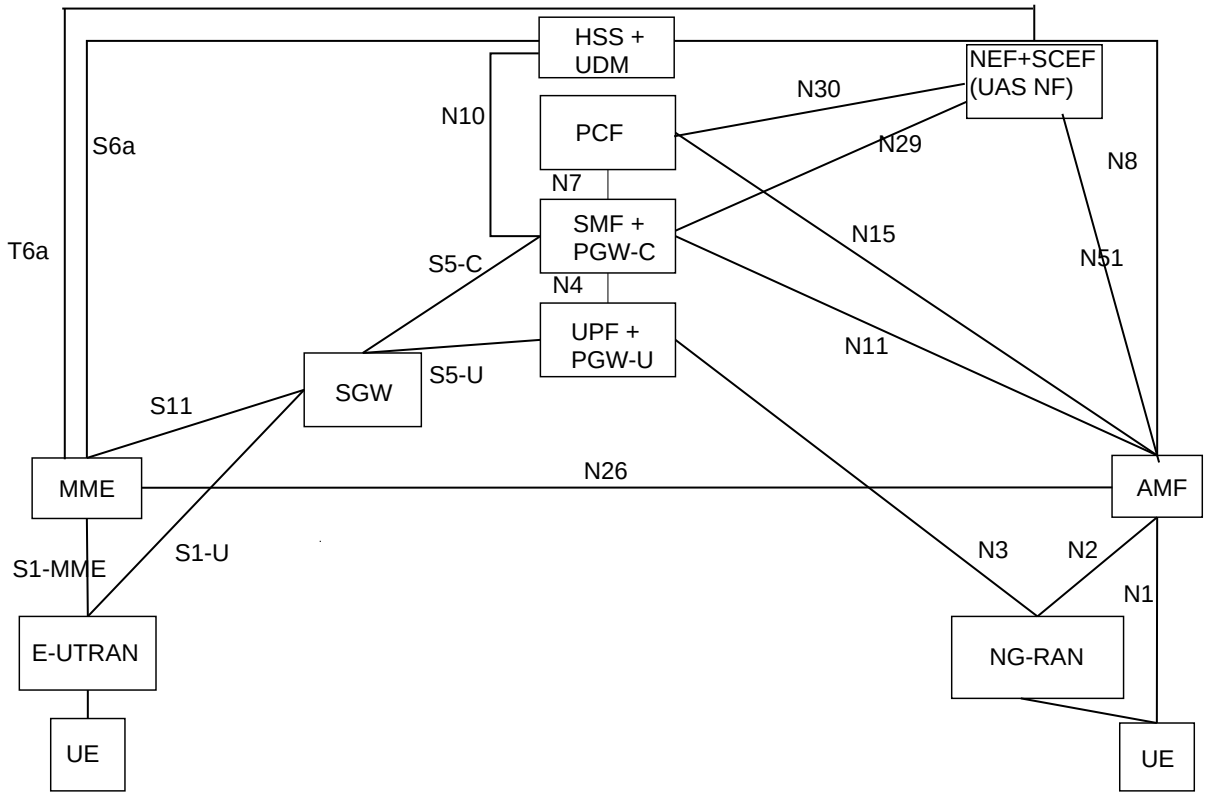

Figure 4.2.2-2: Non-roaming architecture for interworking between 5GS and EPC/E-UTRAN

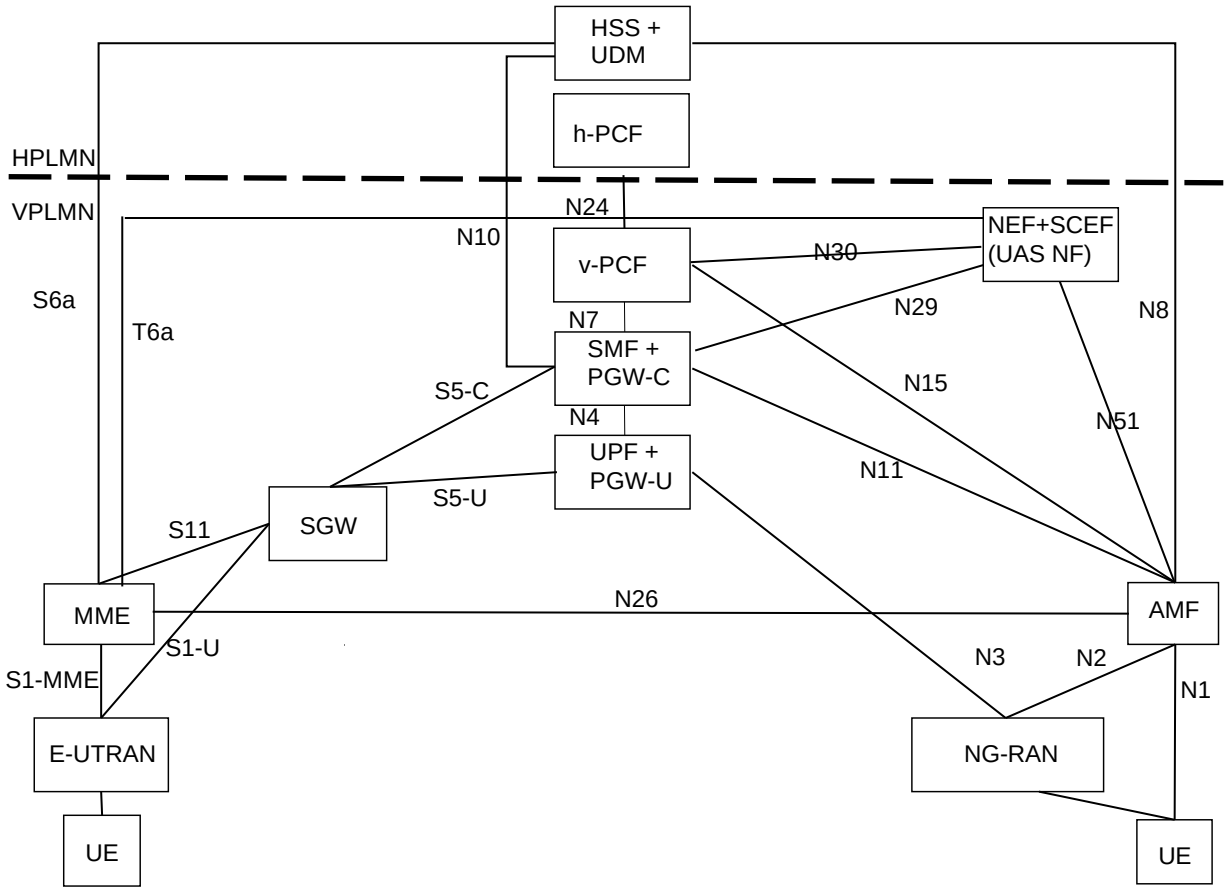

Figure 4.2.2-3: Local breakout roaming architecture for interworking between 5GS and EPC/E-UTRAN

NOTE 2: Transferring the UUAA context from AMF to MME when the UE moves from 5GS to EPS and the UUAA was performed at 5GS registration is not supported on the N26 interface.

NOTE 3: No new UAV-specific functionality is defined for T6a.

4.2.3 5GS Non-roaming Reference Architecture

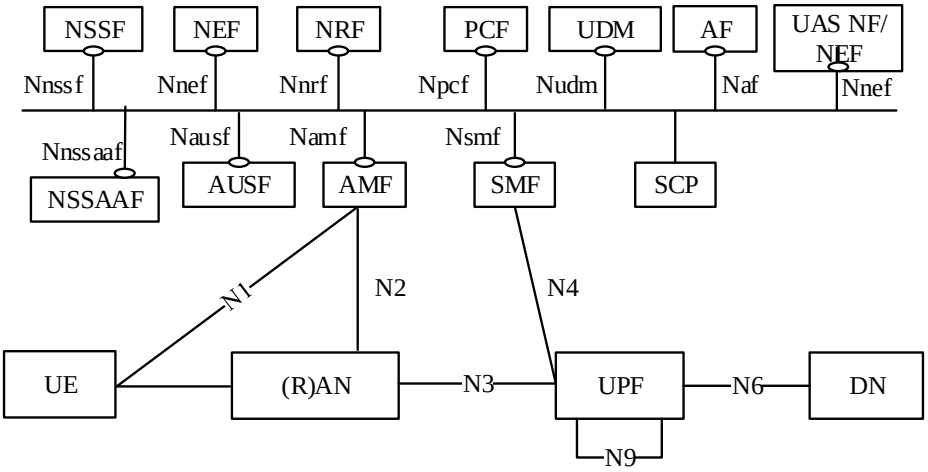

Figure 4.2.3-1: 5G System non-roaming architecture for UAV

4.2.4 5GS Roaming Reference Architecture

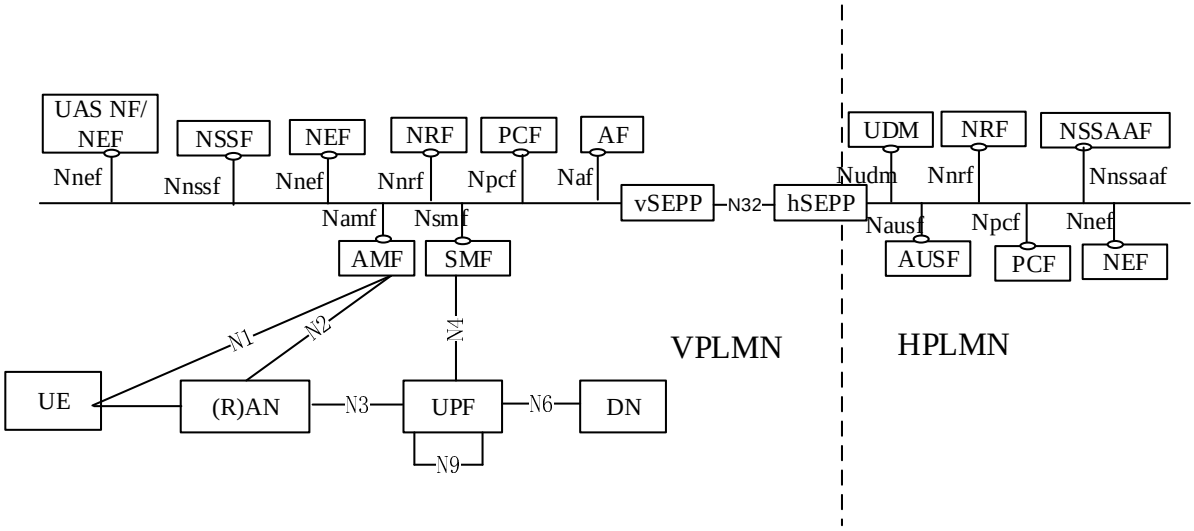

Figure 4.2.4-2: Roaming 5G System architecture for UAV - local breakout scenario in service-based interface representation

4.2.5 Service-based interfaces

The 5G System Architecture for UAVs contains the service-based interfaces defined in TS 23.501 [2].

4.2.6 Reference points

The 5G System Architecture for UAV contains the reference points defined in TS 23.501 [2].

4.3 Functional entities

4.3.1 General

In addition to the 5GS functional entities defined in TS 23.501 [2] and the EPS functional entities defined in TS 23.401 [6], the following functional entities are defined for UAS.

4.3.2 UAS NF

The UAS Network Function is supported by the NEF or SCEF+NEF and used for external exposure of services to the USS. The UAS-NF makes use of existing NEF/SCEF exposure services for UAV authentication/authorization, for UAV flight authorization, for UAV-UAVC pairing authorization, and related re-authentication/re-authorization and revocation; for location reporting, presence monitoring, obtaining list of Aerial UEs in a geographic area and control of QoS/traffic filtering for C2 communication.

The UAS NF may coordinate with the USS to assist CAA-Level UAV ID assignment.

A dedicated NEF may be deployed to provide only the UAS NF functionality, i.e. to support the UAS specific features/APIs and the NEF features/APIs that are specified for capability exposure towards the USS.

For external exposure of services related to specific UAV(s), the UAS NF resides in the VPLMN, in order to interface with country specific USS(es).

When CAPIF is supported by the UAS NF, the UAS NF supports the CAPIF API provider domain functions as specified in TS 23.222 [4].

To support re-authentication/re-authorization and revocation request by USS, the UAS NF stores information as to whether the re-authentication/re-authorization and revocation is towards an AMF or SMF/SMF+PGW-C and the address of the serving AMF or SMF/SMF+PGW-C.

UAS NF stores the result of UUAA-MM procedures and the result of UUAA-SM procedures.

4.3.3 UAV

The UAV is a 3GPP UE supporting the UE functionality defined in TS 23.401 [6] and in TS 23.501 [2].

In addition:

- a UAV that is configured for UAS services is provisioned with a single CAA-Level UAV ID;
- a UAV that is configured for UAS services (i.e. is provisioned with a CAA-Level UAV ID) registers to the 3GPP system for UAS services (i.e. to take advantage of aerial features, connectivity with USS and for C2 connectivity) and provides the CAA-Level UAV ID and a UUAA Aviation Payload to 5GS or EPS. A UAV that has not performed a registration with aviation authorities shall not attempt to request for UAS services.

NOTE: A UAV that is configured for UAS services but does not have an aerial subscription is not allowed by the network to register for UAS services.

4.3.4 AMF

In addition to the functionality defined in TS 23.501 [2], the AMF:

- may trigger the UUAA-MM procedure for a UE requiring UAV authentication and authorization by a USS when registering with 5GS when the UE has Aerial UE subscription information and based on local operator policy, or when the USS that authenticated the UAV triggers a re-authentication, or when AMF itself determines to re-authentication the UAV after the initial registration.

4.3.5 SMF

In addition to the functionality defined in TS 23.501 [2], the SMF:

- triggers the UUAA-SM procedure for a UE requiring UAV authentication and authorization by a USS when requesting user plane resources for UAV operation, or when the USS/UTM that authenticated the UAV triggers a re-authentication;
- may trigger the authorization of pairing between a UAV and a networked UAVC or a UAVC that connects to the UAV via Internet connectivity during the establishment/modification of the PDN connection/PDU session for C2 communication.

4.3.6 SMF+PGW-C

The SMF+PGW-C implements the functions of the SMF described in clause 4.3.5.

4.4 High level function

4.4.1 Service Operations

4.4.1.1 NEF Services

4.4.1.1.1 General

In addition to those defined in TS 23.501 [2] clause 7.2.8 and TS 23.502 [3] clause 5.2.6, the following table illustrates additional NEF services to support UAS.

Table 4.4.2.1.1-1: NF Services provided by NEF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nnef_Authentication	AuthenticateAuthorize	Request/Response	AMF, SMF
	Notification	Subscribe/Notify	AMF, SMF

4.4.1.1.2 Nnef_Authentication service

4.4.1.1.2.1 General

Service Description: This service enables the consumer to either authenticate and authorise, or just authorize, the Service Level Device Identity. In case of UAS, the service is used to authenticate and/or authorize the UAV identified by a CAA-Level UAV ID.

When creating an authentication session, the AMF/SMF implicitly subscribes to NEF about notification related with the authentication/authorization (e.g. re-authenticate, update authorization data or revoke the UUAA authorization). This implicit subscription is implicitly released by UAS NF/NEF when the corresponding authentication association is removed (e.g. in the case of re-authentication failure and USS indicating to release network resource, or in the case of authorization revocation).

4.4.1.1.2.2 Nnef_Authentication_AuthenticateAuthorize service operation

Service operation name: Nnef_Authentication_AuthenticateAuthorize

Description: Provides the authentication and authorization result of the Service Level device Identity.

Input, Required: Service Level Device Identity (i.e. CAA-Level UAV ID) for authentication, GPSI, NF Type.

Input, Conditional Required: Notification endpoint (required for initial authentication request), DNN, S-NSSAI (in case the consumer NF is SMF).

Input, Optional: Authorization Server Address (i.e. USS Address), PEI, UE IP address (in case the consumer NF is SMF), authentication/authorization container provided by UE, UAV location.

Output, Required: None.

Output, Conditional Required: Success/Failure indication [Not required when PDU Session Modification for C2 Communication], Authorization Data container, Indication whether the PDU sessions associated with the "DNN(s) subject to aerial services" can be released [Required for re-authentication failure].

Output, Optional: None.

4.4.1.1.2.3 Nnef_Authentication_Notification service operation

Service operation name: Nnef_Authentication_Notification

Description: Re-authenticate, update authorization data or revoke the UUAA authorization of a UAV.

NOTE: This notification corresponds to an implicit subscription by Nnef_Authentication_AuthenticateAuthorize service operation.

Input, Required: Notification Correlation Information, Service Level Device Identity, 3GPP UAV ID, Notify reason (revoke, re-authentication, or authorization data update).

Input, Conditional Required: Authorization Data container (if the Notify reason is authorization data update).

Input, Optional: None.

Output, Required: Acknowledge indication.

Output, Optional: None.

4.4.1.2 AF Services

4.4.1.2.1 General

In addition to the AF services defined in TS 23.501 [2] clause 7.2.19 and TS 23.502 [3] clause 5.2.19, the following table shows the AF services to support UAS.

Table 4.4.1.2.1-1: NF Services provided by AF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Naf_Authentication	AuthenticateAuthorize	Request/Response	UAS NF/NEF
	Notification	Subscribe/Notify	UAS NF/NEF

4.4.1.2.2 Naf_Authentication service

4.4.1.2.2.1 General

Service Description: This service enables the consumer to authenticate and authorize the Service Level Device Identity. In case of UAS, the service is used to authenticate and authorize the UAV identified by a CAA-Level UAV ID.

When creating an authentication session, the UAS NF/NEF implicitly subscribes to USS about notification related with the authentication/authorization (e.g. re-authenticate, update authorization data or revoke the UUAA authorization). This implicit subscription is implicitly released by USS when the corresponding authentication session is removed (e.g. in the case of re-authentication failure and USS indicating to release network resource, or in the case of authorization revocation).

4.4.1.2.2.2 Naf_Authentication_AuthenticateAuthorize service operation

Service operation name: Naf_Authentication_AuthenticateAuthorize

Description: Provides the Authentication and Authorization result of the Service Level Device Identity (i.e. CAA-Level UAV ID for UAS).

Input, Required: Service Level Device Identity for authentication, GPSI.

Input, Optional: Notification endpoint (required for initial authentication request), PEI, UE IP address, authentication container provided by UE, UAV location.

Output, Required: None.

Output, Conditional Required: Success/Failure indication and GPSI [Not required when PDU Session Modification for C2 Communication], Authorization Data container, Indication whether the UAS service related network resource can be released [Required for re-authentication failure]

Output, Optional: None.

4.4.1.2.2.3 Naf_Authentication_Notification service operation

Service operation name: Naf_Authentication_Notification

Description: Re-authenticate, update authorization data or revoke the UUAA authorization of a UAV.

NOTE: This notification corresponds to an implicit subscription by Naf_Authentication_AuthenticateAuthorize service operation.

Input, Required: Notification Correlation Information, Service Level Device Identity, GPSI, Notify reason (revoke, re-authentication, or authorization data update).

Input, Conditional Required: Authorization Data container (if the Notify reason is authorization data update).

Input, Optional: PDU Session IP address.

Output, Required: Acknowledge indication.

Output, Optional: None.

4.4.1.3 AMF Services

AMF services related to UAS are defined in TS 23.502 [3] clause 5.2.2.

In addition, when SMF invokes Namf_Communication_N1N2MessageTransfer service operation, it may provide the UUAA result to the UAV.

4.4.1.4 SMF Services

SMF services related to UAS are defined in TS 23.502 [3] clause 5.2.8.

4.4.1.5 UDM Services

UDM services related to UAS are defined in TS 23.502 [3] clause 5.2.3.

4.4.1.6 LMF Services

LMF services related to UAS are defined in TS 23.273 [8] clause 8.3.

4.4.1.7 GMLC Services

GMLC services related to UAS are defined in TS 23.273 [8] clause 8.4.

4.4.1.8 UDR Services

UDR services related to UAS are defined in TS 23.502 [3] clause 5.2.12.

4.4.1.9 PCF Services

PCF services related to UAS are defined in TS 23.502 [3] clause 5.2.5.

4.4.2 USS Discovery

There may be multiple USS(es) serving UASs in a country, and no direct association is expected between the 3GPP network serving a UAS and the USS providing services to the UAS. How the association between a UAV and a USS is realized, is outside the scope of 3GPP and is not related to the UAV subscription with the mobile operator.

In order to enable the interaction between the 3GPP network and the USS serving a UAS, the 3GPP network needs to discover the correct USS serving a specific UAV. This is required either during 5GS registration (when the UUAA is performed during 5GS registration), or during PDU session/PDN connection establishment.

It is assumed that mechanisms for resolution of CAA Level UAV ID to the USS serving the corresponding UAV, defined outside 3GPP, and available to entities outside the 3GPP system (e.g. the TPAE), are used in the 3GPP system to discover the USS for the UAV.

Optionally, the UAV may also provide to the 3GPP system, in addition to the CAA-level UAV ID, the USS address or USS FQDN in order to discover the USS for the UAV.

When the UAV provides the USS Address separately from the CAA-Level UAV ID in UUAA-MM or UUAA-SM, the USS Address shall be used to discover the USS. The USS address, when available, is used by the UAS NF in addition to CAA-Level UAV ID to discover a specific USS.

NOTE: A USS, of which the address is provided by the UE, is assumed accessible to any UAS NF/NEF in the 3GPP network.

4.4.3 CAA-Level UAV ID Assignment

The format of the CAA-Level UAV ID is defined outside 3GPP, however how such identity is used to enable a TPAE to query about UAV information is defined with respect to the 3GPP functionality.

In this release, the assignment of a CAA-level UAV ID for Remote Identification functionality applies solely to the UAV. No CAA-level UAV ID is assigned to and used by a UAVC.

Various formats of CAA-level UAV ID must be supported by the UAV to support various geo-specific regulations. At least Serial Number Identification, a CAA-Issued Registration Identifier (aka Session ID), and USS Issued UUID shall be supported.

In the case of Session ID, though the actual format of the CAA-Level UAV ID is defined outside 3GPP and is not decided by 3GPP, it is assumed that the CAA-Level UAV ID used for Remote Identification contains at least the following information:

- an identity unique to the UAV, which may preferably have temporary validity: this identifies uniquely the UAV with the entity that allocates the CAA-level UAV ID.

NOTE 1: Whether privacy or confidentiality requirements will apply to the unique UAV temporary identity depends on regulations in various regions.

- CAA-level UAV ID Routing Information, used by an entity attempting to retrieve the UAV data (e.g. TPAE) to identify and address the appropriate UAS NF/NEF where to send the query. This is also used in USS discovery.

Two types of CAA-level UAV ID assignment are supported:

1. USS-assigned CAA-Level UAV ID: the identity is assigned completely at USS level.

2. 3GPP-assisted CAA-Level UAV ID assignment:

   - The allocation to the UAV of a CAA-Level UAV ID by the USS is done in collaboration with the UAS NF, for the use by the UAV for UUAA, and for the use for Remote Identification.

   - The USS interacts with the UAS NF to allocates the UAV identities to be used for Remote Identification (i.e. the CAA-Level UAV ID). When the UAV registers with the USS before registering to a 3GPP system for

UAS services, the UAV operator provides information about the serving PLMN to the USS. In order to allocate a CAA-Level UAV ID, the USS interacts with a UAS NF if 3GPP Assisted CAA-Level UAV ID Assignment is desired. The 3GPP network selects a UAS NF to respond to the USS, and the UAS NF provides to the USS the CAA-Level Routing Information to enable a resolver of the CAA-level UAV ID to resolve to the UAS NF.

- The USS delegates to the UAS NF the role of "resolver" of the CAA-Level UAV ID and return to an entity (e.g. the TPAE) querying information about the UAV based on the CAA-Level UAV ID the UAV data that the UAS NF retrieves from the USS.

Editor's note: The details of mechanisms of exposure of UAS-NF to entities beyond USS outside the 3GPP system is FFS.

- It is assumed that the mapping between USS assigned CAA-level UAV ID and the associated 3GPP UAV ID is known by the UAS NF after the UAV is authorized by the USS via a successful UUAA. If UAS NF receives a remote identification and tracking query from a TPAE with the USS-assigned CAA-Level UAV ID, the UAS NF uses the mapped 3GPP UAV ID to coordinate with different 3GPP functions to collect the UAV remote identification and tracking information. In addition, the UAS NF can retrieve aviation-level information (e.g. pilot information, USS operator, etc.) from the USS to provide it to the querying party (e.g. TPAE).

NOTE 2: It is assumed that the UAV is not aware of which assignment mechanisms is used for the CAA-Level UAV ID.

4.5 Identifiers

4.5.1 General

The UAV is associated with the following identifiers in the 3GPP system.

4.5.2 CAA-Level UAV Identity

A UAV is assigned a CAA-level UAV Identity by functions in the aviation domain (e.g. USS). This assigned identity is used for Remote Identification and Tracking and to identify the UAV.

The UAV provides the CAA-level UAV Identity to the 3GPP system during UUAA procedures.

The CAA-level UAV Identity is used by the UAV as UAV identity in Remote Identification.

The aviation domain may allocate a new CAA-level UAV Identity for the UAV at any time. The new CAA-level UAV Identity may be provided to the UAV and 3GPP system during UAS related procedures.

NOTE: It is assumed that mechanisms are available to ensure privacy and protection (e.g. anti-spoofing) of the CAA-assigned UAV Identity when it is used for Remote Identification. Security solutions to provide such privacy are outside the scope of this specification.

4.5.3 3GPP UAV ID

A 3GPP UAV ID is associated to the UAV by the 3GPP system in the subscription information and is used by the 3GPP system to identify the UAV. GPSI in the format of External Identifier is used as the 3GPP UAV ID.

The USS stores the association of the CAA-level UAV ID (provided by the UAV or a new one allocated by the aviation domain) to the 3GPP UAV ID (which is provided during the UUAA procedure).

5 Functional description and information flows

5.1 Control and user plane stacks

Editor's note: This clause will describe the protocol stacks on the control and user planes for each of the interfaces required for UAS.

5.2 UAV Authentication and Authorization

5.2.1 UUAA Model

The following applies for UUAA for a UAV:

- UUAA-MM is optional and performed at 5GS registration based on operator's policy. If required by the operator, UUAA-MM is performed if the UAV has an aerial UE subscription in the Access and Mobility Subscription Data and provides the CAA-Level UAV ID in the Registration Request message.

- UUAA-SM in 5GS is performed at PDU session establishment to a subscribed DNN applicable for UAS services if the UAV provides the CAA-Level UAV ID in the PDU Session Establishment Request message. Whether the DNN is applicable for UAS services is determined by the aerial service indication being set for the DNN in the Session Management Subscription Data.

- UUAA-SM in EPS is performed at PDN Connection Establishment when activating a PDN Connection to a subscribed APN applicable for UAS service if the UAV provides the CAA-Level UAV ID in the ESM container. Whether the APN is applicable for UAS services is determined by the aerial service indication being set for the corresponding DNN in the Session Management Subscription Data (fetched from UDM triggered by CAA-Level UAV ID being provided in request).

- UUAA-SM may be performed to re-authenticate the UAV or to reauthorize at PDU session modification or EPS bearer modification (e.g. in case of C2 authorization or flight plan authorization change) if the UE includes CAA-Level UAV ID and a UUAA Aviation Payload.

NOTE: If the network is configured to perform UUAA at registration, UAV has not provided CAA-Level UAV ID and the UE has aerial subscription, then the AMF can allow the UAV to register as a normal UE. If the network is configured to perform UUAA at PDU Session Establishment, the UE has not provided CAA-Level UAV ID and the SM subscription data indicates that UUAA-SM to be performed, the SMF rejects the PDU Session Establishment request.

5.2.2 UUAA at Registration in 5GS (UUAA-MM)

5.2.2.1 General

The UUAA-MM procedure is optional and triggered for a UE that requires UAV authentication and authorization by a USS when registering with 5GS. The UUAA-MM procedure is triggered by the AMF. UUAA-MM is triggered during the UE Registration based on the local network policy, if the UE has an Aerial UE subscription with the 5GS and if the UE has provided the CAA-Level UAV ID of the UAV in the Registration Request, or when the USS that authenticated the UAV triggers a re-authentication.

The UE is authenticated and authorized by USS using a CAA-Level UAV ID and credentials associated to the CAA-Level UAV ID, different from the 3GPP subscription credentials (e.g. SUPI and credentials used for PLMN access). During UUAA-MM procedure, the AMF communicates with the USS via a UAS NF and forwards authentication messages transparently between the UE and UAS NF.

UAS NF stores the UAV UEs UUAA context after successful UUAA procedure. The UUAA context may be stored in the UDSF or may be stored locally in the UAS NF depending on deployments. The UAS NF shall also create an implicit subscription for notification towards the AMF after the successful UUAA procedure. This notification is used

by the UAS NF to trigger re-authentication, update authorization data or revoke authorization of the UAV, upon receipt of such request from the USS.

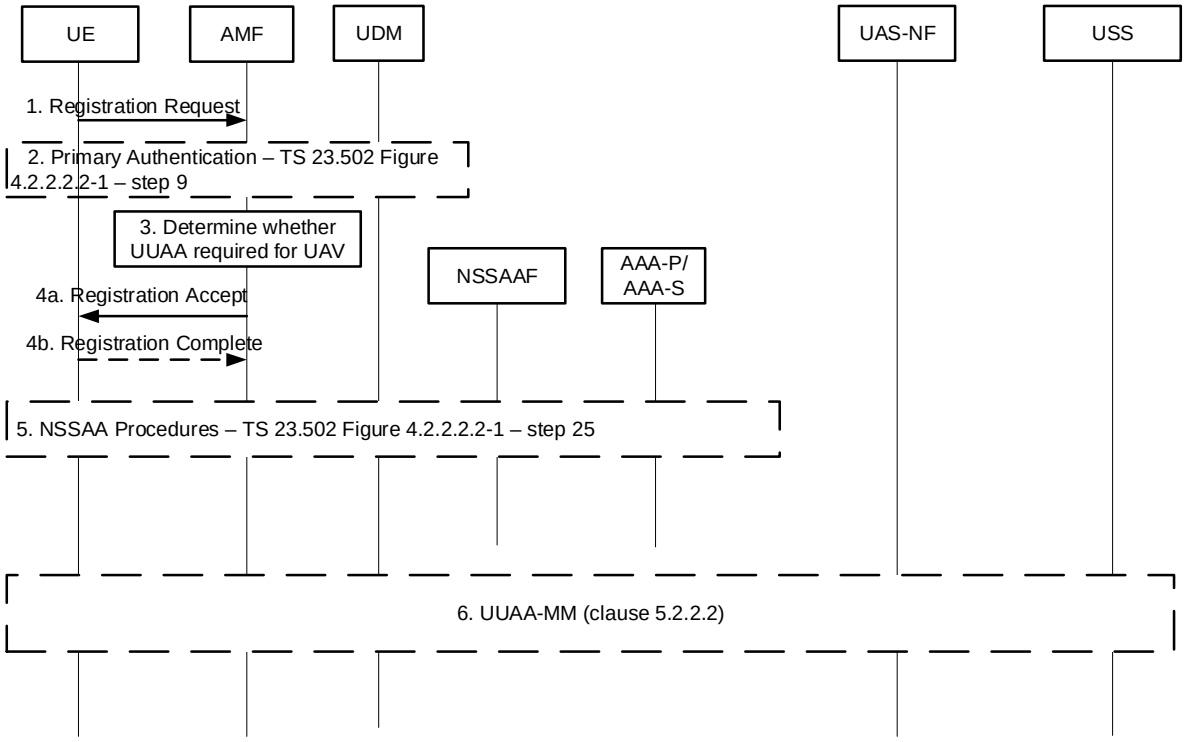

Figure 5.2.2.1-1: UUAA in the context of the Registration procedure (UUAA-MM)

1. The UE sends a Registration request message and, if configured with one, it shall provide a CAA-level UAV ID of the UAV and optionally a USS address when registering for UAS services.

2. If primary authentication is required (e.g. if this is an initial Registration), AMF invokes it as described in step 9 in Figure 4.2.2.2.2-1 of TS 23.502 [3]. Subsequently AMF retrieves UE subscription data from UDM as described in step 14 in Figure 4.2.2.2.2-1 of TS 23.502 [3] - (not shown in the figure).

3. AMF shall determine whether UUAA-MM is required for the UAV. The AMF decides that UUAA is required if:

   a) the UE has a valid Aerial UE subscription information;

   b) UUAA is to be performed during Registration according to local operator policy;

   c) there is no successful UUAA result from a previous UUAA-MM procedure;

   d) the UE has provided a CAA-Level UAV ID.

   AMF shall not perform UUAA-MM for non-3GPP access and shall ensure that the UE is not allowed to access any aerial services in non-3GPP access by rejecting PDU session establishment requests for aerial services (identified by DNN/S-NSSAI).

4. If AMF determines in step 3 that a UUAA-MM is to be performed, AMF shall include a pending UUAA-MM indication in the Registration Accept message. The AMF stores in the UE context that a UUAA is pending. The UE shall wait for completion of the UUAA-MM procedure without attempting to register for UAS services or to establish user plane connectivity to USS or UAV-C.

   If AMF determines that UUAA is not to be performed during this Registration procedure, UUAA may be triggered during PDU Session Establishment later on.

   If UUAA is configured in the AMF to be performed during 5GS registration and the UE has provided a CAA-Level UAV ID in the registration request in step 1, but the UE does not have an aerial subscription in the UE subscription data retrieved from the UDM in step 2, then the AMF rejects the registration with an indication informing no aerial subscription. This information indicates to the UAV of the reason for the rejection for aerial services and ensures that the UE is not allowed to access any aerial service.

If UAS services become enabled or disabled (e.g. because the aerial subscription becomes a part of the UE subscription data retrieved from UDM as described in clause 5.2.3.3.1 of TS 23.502 [3]) then AMF may trigger a UE Configuration Update procedure as described in clauses 4.5.1 and 4.2.4.2 of TS 23.502 [3] to notify the UE. The UE may initiate a mobility registration update procedure to get the UAS services after completion of the UE Configuration Update procedure.

If UUAA is configured in the AMF to be performed during 5GS registration, the UE did not provide a CAA-Level UAV ID in the registration request in step 1, but UE has aerial subscription in the UE subscription data retrieved from UDM in step 2, then the AMF accepts the registration and ensures that the UE is not allowed to access any aerial service by storing in the UE context that 'UUAA-MM has FAILED', and further rejecting PDU session establishment requests for aerial services (identified by DNN/S-NSSAI). At a later point in time, if the UE wants to use the aerial services by providing the CAA Level UAV ID later on via UUAA-MM procedure, then the UE shall first perform Mobility Registration Update as explained in clause 4.2.2.2.2 of TS 23.502 [3].

5. If UE indicates its support for Network Slice-Specific Authentication and Authorization (NSSAA) procedure in the UE MM Core Network Capability, and if the UE includes Requested S-NSSAI in Registration Request which is subject to NSSAA, however, the Requested S-NSSAI has not been successfully authenticated, the NSSAA procedure is executed as described in clause 4.2.2.2.2 of TS 23.502 [3].

6. If required based on step 3 determination, and if the S-NSSAI that is associated with the UAS services is part of the Allowed NSSAI, UUAA-MM procedure (see clause 5.2.2.2) is executed at this step. Once the UUAA-MM procedure is successfully completed for the UAV, the AMF stores a successful UUAA result and updates the UE context indicating that UUAA is no longer pending and the authorized CAA-Level UAV ID if provided by the USS. The USS may provide a new CAA-Level UAV ID as the authorized CAA-Level UAV ID. The AMF shall trigger a UE Configuration Update procedure (see TS 23.502 [3], clause 4.2.4.2) to deliver the UUAA result, the UUAA Authorization Payload containing UAV configuration and the authorized CAA-Level UAV ID if received from the USS to the UE.

NOTE 1: The UAV configuration is application layer information outside the scope of 3GPP.

If UUAA fails, based on local network policy, the AMF may decide to de-register the UE with an appropriate cause value in the De-Registration Request message, or keep the UE-registered with a failure UUAA result in UE context as described in step 7 of clause 5.2.2.2 and ensures that the UE is not allowed to access any aerial service based on the DNN/S-NSSAI value. If the UE is de-registered, the UE may re-attempt to re-register without including the CAA-level UAV ID.

NOTE 2: The security aspects for this procedure is defined in TS 33.256 [10].

5.2.2.2 UUAA-MM Procedure

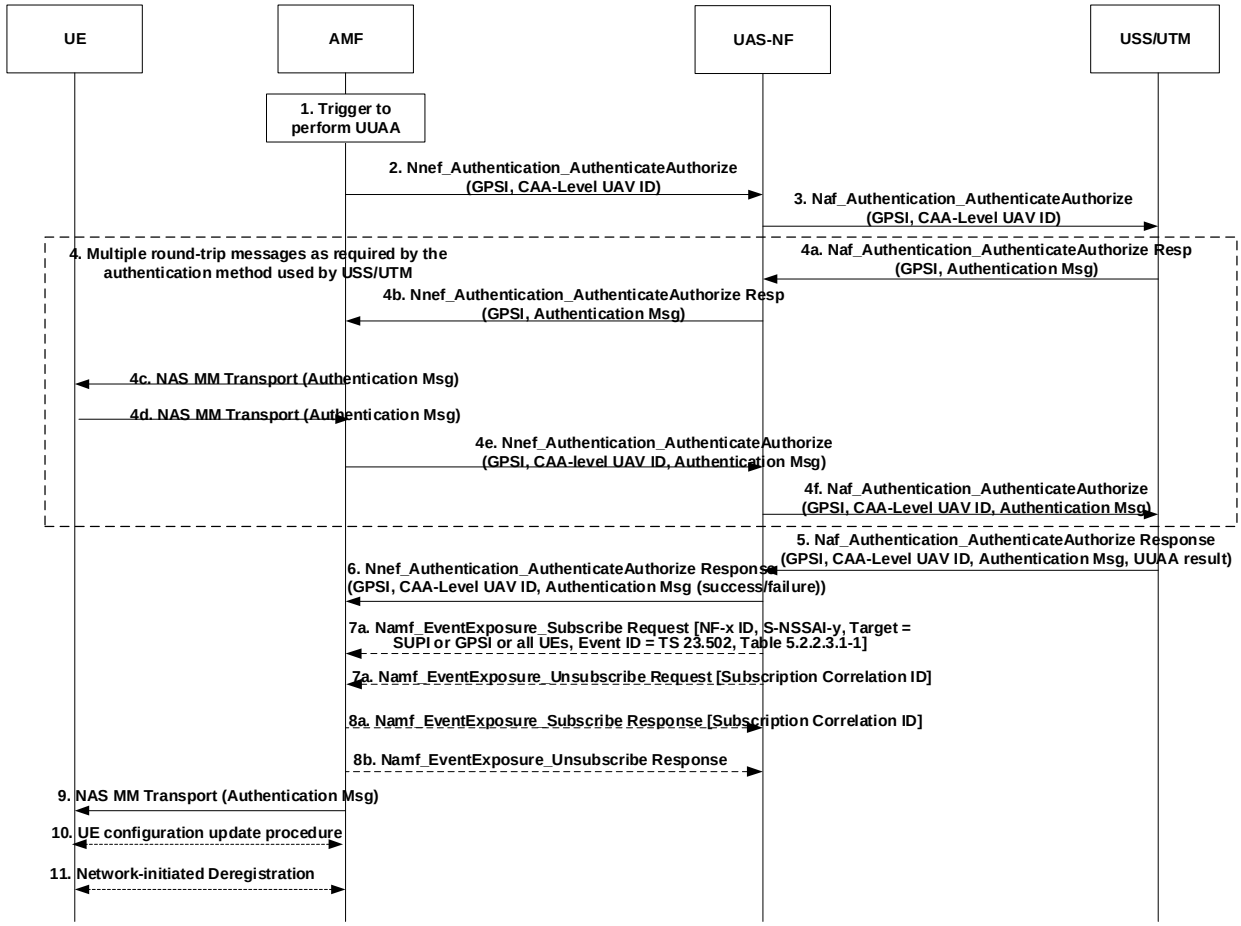

Figure 5.2.2.2-1: UUAA-MM procedure

1. For a UE that requires UUAA or when triggered by re-authentication by USS, the AMF triggers a UUAA-MM procedure. If the UE does not have an Aerial subscription in the UE subscription data retrieved from the UDM, the AMF shall not trigger a UUAA-MM procedure.

2. AMF to UAS NF/NEF: The AMF invokes Nnef_Authentication_AuthenticateAuthorize Request message. For initial authentication, this shall include the GPSI and the CAA-Level UAV ID and may include USS address (e.g. FQDN), UUAA Aviation Payload if it was provided by the UE. For re-authentication triggered by AMF, this may not include the CAA-Level UAV ID. UAS NF resolves the USS address based on CAA-Level UAV ID or uses the provided USS address, as described in clause 4.4.2. In addition, the AMF may also include the User Location Information (e.g. Cell ID). The UAS NF should store the serving AMF ID.

   The AMF identifies the UAS NF/NEF based on local configuration or by NF discovery procedure using DNN/S-NSSAI and/or UE provided identity e.g. USS address.

   The AMF also provides a Notification Endpoint to the UAS NF/NEF, so that UAS NF/NEF can include this Notification Endpoint together with UUAA updated parameters, as shown in clause 5.2.4. By providing the Notification Endpoint, the AMF is implicitly subscribed to be notified of re-authentication, update authorization data or revocation of UAV from UAS NF/NEF, if the UUAA result is successful in step 5.

NOTE 1: The security aspects for this procedure is defined in TS 33.256 [10].

3. UAS NF/NEF to USS: Naf_Authentication_AuthenticateAuthorize Request message, shall include the GPSI and CAA-Level UAV ID and optionally UAV location obtained from AMF in step 2 e.g. to support geo-caging functionality. UAS NF/NEF may translate the Cell ID received as UAV location from AMF in step 2 into a corresponding geographic area and/or may further obtain the UE location information using Location Service Procedures as defined in TS 23.273 [8].

The UAS NF/NEF also provides a Notification Endpoint to the USS, so that USS can include this Notification Endpoint together with UUAA updated parameters, as shown in clause 5.2.4. By providing the Notification Endpoint, the UAS NF/NEF is implicitly subscribed to be notified of re-authentication, update authorization data or revocation of UAV from USS, if the UUAA result is successful in step 5.

4. [Conditional] Multiple round-trip messages as required by the authentication method used by USS. Naf_Authentication_AuthenticateAuthorize Response messages from USS shall include GPSI and shall include a authentication message based on authentication method used that is forwarded transparently to UE over NAS MM transport messages. The authentication message in step4d may contain UUAA Aviation Payload required by the USS if it was not provided by the UE before.

5. USS to UAS NF/NEF: (final) Naf_Authentication_AuthenticateAuthorize Response message, shall include: GPSI, a UUAA result (success/failure) for the UAV and the UAS NF, may include an authorized/new CAA-Level UAV ID for the UAV and a UUAA Authorization Payload to the UAV (e.g. security info to be used to secure communications with USS), and a final authentication message (e.g. indicating success or failure, and if the UUAA is for re-authentication, indicating whether the UAS service related network resource can be released in case of UUAA failure) based on authentication method used that is forwarded transparently to UE over NAS MM transport messages.

6. UAS NF/NEF to AMF: (final) Nnef_Authentication_AuthenticateAuthorize Response message, forwards information received from USS in step 5. If UUAA for re-authentication failed and UAS NF/NEF received indication that the UAS service related network resource can be released in step 5, the UAS NF/NEF includes an indication that the PDU sessions associated with the "DNN(s) subject to aerial services" can be released.

7a. [Conditional] UAS NF/NEF to AMF: If UUAA-MM succeeded and UAS NF/NEF has not subscribed to AMF for the Mobility Event Exposure before, UAS NF/NEF subscribes to AMF for the mobility event notification by sending Namf_EventExposure_Subscribe request with the mobility events as described in TS 23.502 [3], Table 5.2.2.3.1-1 with Event ID = Reachability Filter.

7b. [Conditional] UAS NF/NEF to AMF: If UUAA-MM failed and UAS NF/NEF has subscribed to AMF for the Mobility Event Exposure earlier, UAS NF/NEF unsubscribes to AMF for the mobility event notification by sending Namf_EventExposure_Unsubscribe request with Subscription Correlation ID.

8a. [Conditional] AMF to UAS NF/NEF: The AMF acknowledges the subscription request from 7a by sending Namf_EventExposure_Subscribe response with Subscription Correlation ID.

8b. [Conditional] AMF to UAS NF/NEF: The AMF acknowledges the un-subscription request from 7b by sending Namf_EventExposure_Unsubscribe response.

9. AMF to UE: (final) NAS MM transport message forwarding authentication message from USS including authentication/authorization result (success/failure).

10. [Conditional] if UUAA-MM succeeded, AMF triggers a UE Configuration Update procedure to deliver to the UAV authorization information from USS, as described in clause 5.2.2.1.

11. [Conditional] If UUAA-MM fails during a Re-authentication and Re-authorization and there are PDU session(s) established using UAS services, and the USS has indicated that the network resources can be released, AMF may trigger these PDU Sessions release. AMF identifies the relevant PDU session(s) for UAS services based on the DNN/S-NSSAI value of the PDU session.

NOTE 2: When the UUAA-MM fails during a Re-authentication, and the USS has not indicated that the network resources can be released, the USS can initiate UUAA revocation as described in clause 5.2.7.

[Conditional] if UUAA-MM fails, based on network policy the AMF may trigger Network-initiated Deregistration procedure described (as specified in clause 4.2.2.3.3 of TS 23.502 [3]) and it shall include in the explicit De-Registration Request the appropriate rejection cause value.

If there is an AMF relocation for the UAV, the new serving AMF shall notify the UAS NF about the new AMF ID and the related CAA-level UAV ID using the existing AMF event notification service.

At any time after the initial registration, the USS (via UAS NF/NEF) or the AMF may initiate Re-authentication procedure for the UAV. For AMF initiated case the Re-authentication procedure shall start from step 2. USS initiated re-authentication procedure is described in clause 5.2.4.

If the UE is deregistered as per clause 4.2.2.3 of TS 23.502 [3], then the AMF shall unsubscribe to UAS NF and then UAS NF/NEF may clear the UUAA-MM context and update USS.

5.2.3 UUAA At PDN Connection/PDU Session Establishment (UUAA-SM)

5.2.3.1 General

NOTE 1: The security aspects for this procedure is defined in TS 33.256 [10].

An UAV uses PDU Sessions or PDN Connections in the UE for connectivity with the USS and for connectivity with a networked UAV-C.

A networked UAV-C is a UE which uses existing procedures for establishing PDU Session or PDN Connection for communication with the USS/UTM, and the procedures described in this clause do not apply to a networked UAV-C.

This clause describes procedure that applies both for 5GS and EPS, where PDU Session refers to 5GS and PDN Connection refers to EPS.

PDU Session(s)/PDN Connection(s) for UAS services shall only be established after a UAV has been authenticated and authorized by the USS. This may happen during UUAA-SM as described in this clause.

A UAV may use either a common or separate PDU Session/PDN connection for connectivity with the USS and a UAV-C.

When the UAV requests establishment of a PDU session/PDN connection, the PDU session/PDN Connection may require UUAA authorization of the UAV, subject to operator policy and regulatory requirements.

If the UAV uses the PDU session/PDN connection for C2 the PDU session is subject to C2 authorization as described in clause 5.2.5.

The PDU Session/PDN Connection is identified by the SMF/SMF+PGW-C as being for USS/C2 communication based on the aerial service indication set in the Session Management Subscription data for the DNN or DNN and S-NSSAI combination.

To subscribe to the PDU Session/PDN Connection Status Event, UAS NF/NEF determines the APN/DNN or DNN and S-NSSAI combination as below:

- The UAS NF/NEF may receive APN/DNN or DNN and S-NSSAI combination from the USS as specified in clause 4.15.3.2.3 of TS 23.502 [3];
- The UAS NF/NEF may map the AF-Identifier from the USS into APN/DNN or DNN and S-NSSAI combination based on local configuration as specified in clause 4.15.3.2.3 of TS 23.502 [3]; or
- The UAS NF/NEF may map the External Application Identifier from the USS into the APN/DNN or DNN and S-NSSAI combination based on local configuration.

NOTE 2: If the PDU session/PDN connection for C2 communication and the PDU session/PDN connection for USS communication are separate, different AF-Identifiers or External Application Identifiers can be used.

During the establishment or modification procedure of the PDU Session/PDN connection for C2 communication, the USS shall provide the 3GPP system with following information for enabling basic C2 communication between UAV and UAV-C:

- Traffic filters;
- QoS requirements.

The USS can enable/disable C2 communication between UAV and UAV-C necessary for services used during the flight operation at any point in time as described in clause 5.2.9.

UAS NF stores the UAV UEs UUAA context after successful UUAA-SM procedure. The UUAA context may be stored in the UDSF or may be stored locally in the UAS NF depending on deployments. The SMF shall subscribe for notifications from UAS NF which may be used to trigger re-authentication, update authorization data or revoke authorization of the UAV, upon receipt of such request from the USS.

Clause 5.2.3.2 defines the USS UAV Authorization/Authentication (UUAA) procedures at PDU Session Establishment in 5GS and clause 5.2.3.3 is for the PDN Connection Establishment in the Attach procedure for EPS using the interworking functionality.

When the C2 authorization is revoked by the USS, the SMF or SMF+PGW-C shall release the PDU Session/PDN connection for C2 communication (in case separate PDU Sessions/PDN Connections are used), or disable C2 communication for the PDU Session/PDN connection (in case common PDU Session/PDN Connection is used), e.g. by removing the traffic filters for C2 communications and the QoS flow for C2 communication, and informs the UE with a PDU session modification/bearer modification request.

When the UUAA is revoked by the USS, all UAV related PDU Session/PDN connections shall be released.

5.2.3.2 USS UAV Authorization/Authentication (UUAA) during the PDU Session Establishment

The USS UAV Authorization/Authentication (UUAA) is triggered by the SMF during the PDU Session Establishment, specified in TS 23.502 [3], clause 4.3.2.2 and additionally based on the SM subscription data obtained from UDM, and the Service Level Device Identity provided by the UE in the PDU Session establishment request.

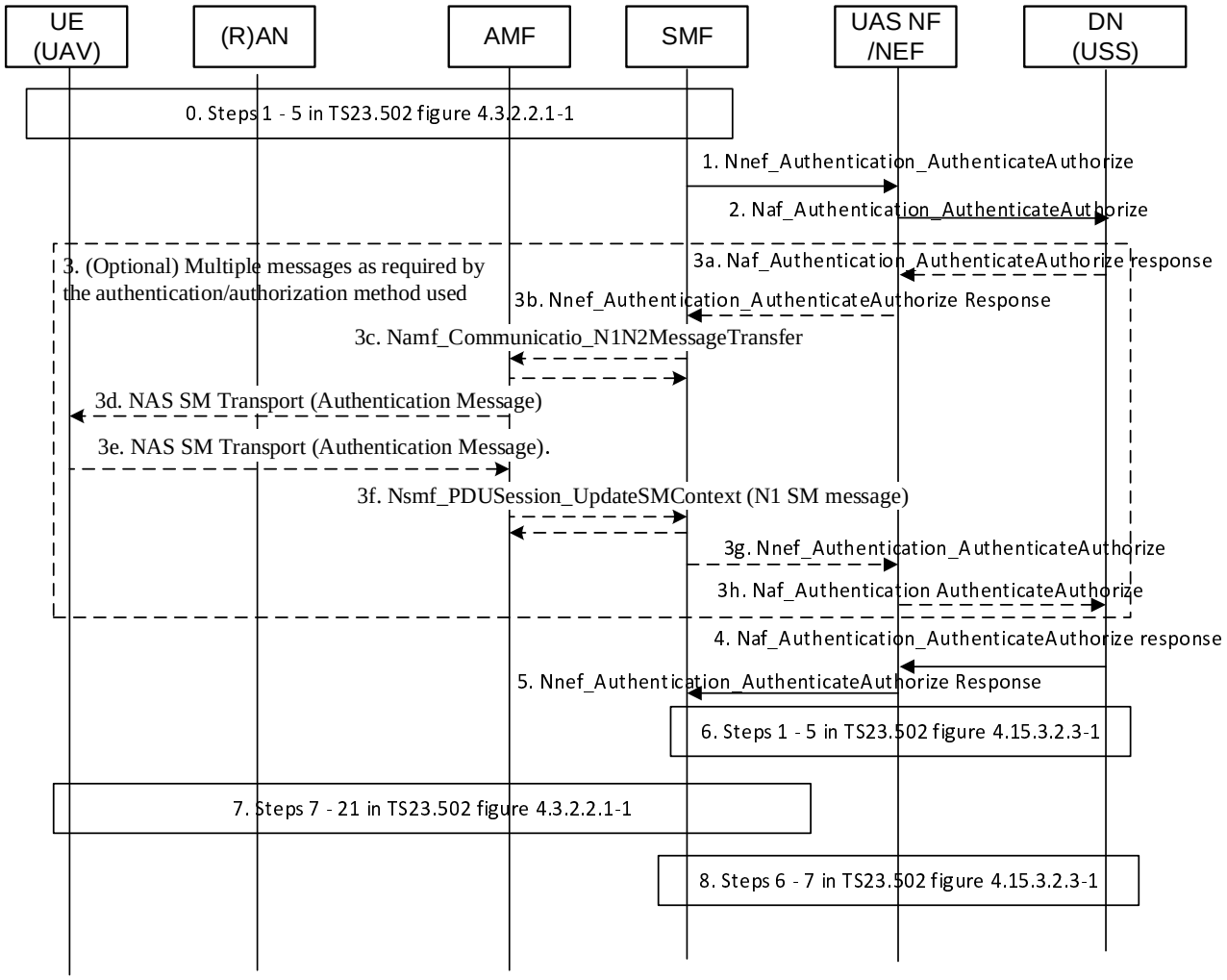

Figure 5.2.3.2 -1: UUAA during PDU Session Establishment

The procedure assumes that the UE/UAV has already registered on the AMF.

0. Steps 1 - 5 as in TS 23.502 [3] figure 4.3.2.2.1-1.

   The UAV includes the Service Level Device Identity (e.g. the CAA-Level UAV ID of the UVA) and may include the Authentication Server Address (i.e. the USS address) and optionally Authentication Data (i.e. the UUAA Aviation Payload) in the PDU Session Establishment request.

The SMF determines that it needs to invoke UAS NF/NEF service operation for UUAA Authentication/Authorization of the PDU session establishment request based on that the provided DNN/S-NSSAI combination is dedicated for aerial services (have aerial service indicator set) and that the Service Level Device Identity (CAA-Level-UAV ID) is included in the request. If the provided APN/DNN is dedicated for aerial services but Service Level Device Identity (CAA-Level UAV ID) is not provided, the SMF shall reject the establishment of the PDU Session and steps 1 - 9 are not performed.

The SMF identifies the UAS NF/NEF based on local configuration or by NF discovery procedure using DNN/S-NSSAI and/or UE provided identity e.g. USS address.

1. The SMF invokes Nnef_Authentication_AuthenticateAuthorize service operation, including the Service Level Device Identity (that contains the CAA-Level UAV ID of the UAV), DNN, S-NSSAI, and may include the Authentication Server Address (i.e. the USS address) and the UUAA Aviation Payload if it was provided by the UE, GPSI, optionally UAV location, PEI if available, and the UE IP Address if available. The UAV location is the User Location Information provided by the AMF (e.g. Cell ID). The UAS NF/NEF selects a USS based on either the Service Level Device Identity (i.e. CAA-Level UAV ID of the UAV) or the Authentication Server address (i.e. USS address) as described in clause 4.4.2.

   SMF also provides a Notification Endpoint to the UAS NF/NEF, so that UAS NF/NEF can include this Notification Endpoint together with UUAA updated parameters, as shown in clause 5.2.4. By providing the Notification Endpoint, the SMF is implicitly subscribed to be notified of re-authentication, update authorization data or revocation of UAV from UAS NF/NEF, if the UUAA result is successful in step 4.

2. From UAS NF/NEF to USS: Naf_Authentication_AuthenticateAuthorize service operation forwarding the authentication request received information from the SMF. UAS NF may translate the Cell ID received as part of UAV location in the Nnef_Authentication_AuthenticateAuthorize request at step 1 into a corresponding geographic area and/or may further obtain the UE location information using Location Service Procedures as defined in TS 23.273 [8] and include them in the Naf_Authentication_AuthenticateAuthorize message towards the USS e.g. to support geo-caging functionality.

   UAS NF/NEF also provides a Notification Endpoint to the USS, so that USS can include this Notification Endpoint together with UUAA updated parameters, as shown in clause 5.2.4. By providing the Notification Endpoint, the UAS NF/NEF is implicitly subscribed to be notified of re-authentication, update authorization data or revocation of UAV from USS, if the UUAA result is successful in step 4.

3. [Conditional] Multiple round-trip messages as required by the authentication method used by USS. This step is performed if the Naf_Authentication_AuthenticateAuthorize response messages from USS in step 3a does not contain a UUAA result (SUCCESS/FAILURE). Naf_Authentication_AuthenticateAuthorize response messages from USS shall include GPSI and shall include an authentication message based on authentication method used that is forwarded transparently to UE over NAS MM transport messages. The authentication message in step3e may contain UUAA Aviation Payload required by the USS if it was not provided by the UE before.

4. From USS to UAS NF/NEF: Naf_Authentication_AuthenticateAuthorize response.

   The USS sends Naf_Authentication_AuthenticateAuthorize response to the UAS NF/NEF with the Authentication/Authorization result containing the UUAA result (SUCCESS/FAILURE) for the UAS NF and indication whether the UAS service related network resource can be released in the case of UUAA failure for re-authentication or re-authorization, optionally a Service Level Device Identity containing the authorized CAA-Level UAV ID, requested policy information and the UUAA Authorization Payload. The requested policy information from USS may contain a DN Authorization Profile Index and/or a DN authorized Session AMBR. The USS may include a new CAA-Level UAV ID as authorized CAA-Level UAV ID.

NOTE 1: The USS stores a mapping between CAA-Level UAV ID and the External Identifier (i.e. GPSI as defined in clause 4.5.3). The External Identifier (GPSI) and/or UAV IP Address can be used at a later point by the USS for accessing various services exposed by 3GPP network e.g. location information retrieval, monitoring event configuration, requesting dedicated policies for e.g. C2, etc.

5. The UAS NF/NEF confirms the successful Authentication/Authorization of the PDU Session. The UAS NF/NEF stores the UUAA result together with the GPSI. UAS NF/NEF forwards the Authentication/Authorization result, a Service Level Device Identity containing the authorized CAA-Level UAV ID and the Authorization Data (i.e. the UUAA Authorization Payload), if received from the USS, to the SMF.

6. [Conditional] If the authentication/authorization is successful, the USS shall subscribe to the PDU Session Status Event as described in steps 1-5 in Figure 4.15.3.2.3-1 of TS 23.502 [3]. This step can be executed in parallel to

step 4. The UAS NF/NEF determines the DNN, S-NSSAI to subscribe to the PDU Session Status Event notification as specified in clause 5.2.3.1.

7. The PDU Session establishment continues with steps 7 to 21 in Figure 4.3.2.2.1-1 of TS 23.502 [3] and completes. In the step 7b in Figure 4.3.2.2.1-1of TS 23.502 [3], if the SMF receives the DN Authorization Profile Index from the UAS NF/NEF, it sends the DN Authorization Profile Index to retrieve the PDU Session related policy information (described in clause 6.4 of TS 23.503 [9]) and the PCC rule(s) (described in clause 6.3 of TS 23.503 [9]) from the PCF. If the SMF receives the DN authorized Session AMBR in from the UAS NF/NEF, it sends the DN authorized Session AMBR within the Session AMBR to the PCF to retrieve the authorized Session AMBR (described in clause 6.4 of TS 23.503 [9]).

   The SMF transfers the Authentication/Authorization result, the Service Level Device Identity containing the authorized CAA-Level UAV ID and the Authorization Data (i.e. the UUAA Authorization Payload) to the UAV if received from the UAS NF, as in steps 11, 12 and 13 in figure 4.3.2.2.1-1 of TS 23.502 [3].

   If the authentication/ authorization result is a failure, the SMF rejects the PDU session establishment with a proper cause value.

8. [Conditional] If the USS in step 6 subscribed to the PDU Session Status Event the SMF will, as described in steps 6-7 in Figure 4.15.3.2.3-1 of TS 23.502 [3], detect when the PDU Session is established, and send the PDU Session Establishment event report to the UAS NF/NEF by means of Nsmf_EventExposure_Notify message, including GPSI and the UE IP Address. Then, the UAS-NF/NEF forwards the event message to the USS.

If UUAA-SM fails during a Re-authentication and Re-authorization and the USS has indicated that the network resources can be released, SMF may trigger PDU Session release for UAS services with a proper cause value.

NOTE 2: When the UUAA-SM fails during a Re-authentication, and the USS has not indicated that the network resources can be released, the USS can initiate UUAA revocation as described in clause 5.2.7.

NOTE 3: If C2 information reference is available from USS during the initial PDU Session Establishment procedure the SMF can interact with the PCF to set up a predefined PCC rule(s) profile for the C2 communication.

If the PDU session is released as per clause 4.3.4 of TS 23.502 [3] then the SMF shall unsubscribe to UAS NF/NEF and then UAS NF/NEF may clear the UUAA-SM context and update USS.

5.2.3.3 USS UAV Authorization/Authentication (UUAA) during default PDN connection at Attach

In the figure 5.2.3.3-1 the execution of the UUAA is specified.

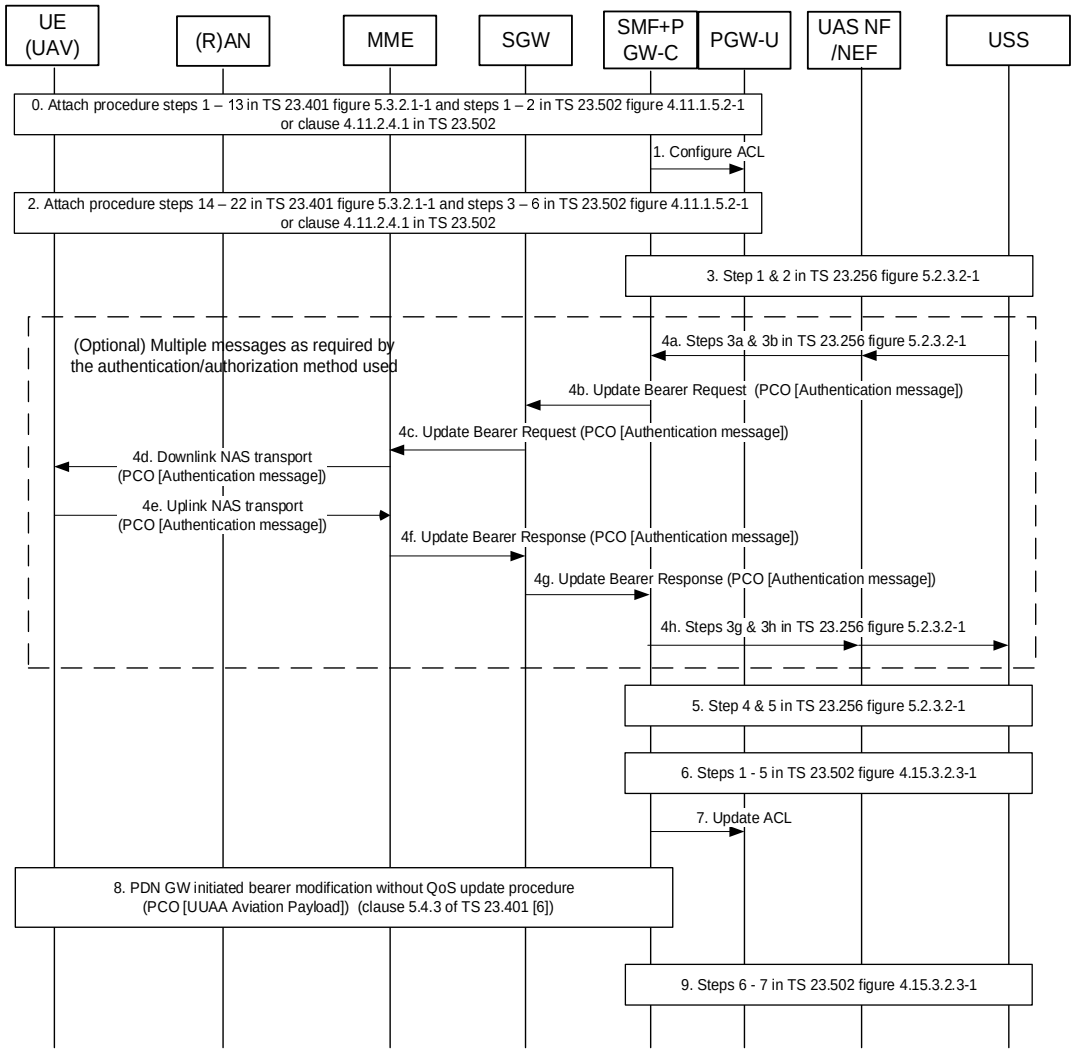

Figure 5.2.3.3-1: UUAA during PDN connection establishment at Attach procedure in EPS

0. Steps 1 - 13 in TS 23.401 [6] figure 5.3.2.1-1 and steps 1 - 2 in TS 23.502 [3] figure 4.11.1.5.2-1 or clause 4.11.2.4.1 in TS 23.502 [3].

   UE sends Attach Request including the Service Level Device Identity (i.e. the CAA-Level UAV ID of the UAV), and may include the Authentication Server Address (i.e. the USS address) and optionally Authentication Data (i.e. the UUAA Aviation Payload), etc. in the PCO to the SMF+PGW-C.

   Based on that the Service Level Device Identity (CAA-Level UAV ID) is provided with the request, the SMF+PGW-C retrieves the Session Management Subscription Data from the UDM+HSS using the Nudm_SDM_Get service operation, and based on that the provided APN/DNN is dedicated for aerial services (have aerial service indicator set), it determines to invoke UAS NF/NEF service operation for UUAA Authentication/Authorization. If the provided APN/DNN is dedicated for aerial services but Service Level Device Identity (CAA-Level UAV ID) is not provided, the SMF+PGW-C shall reject the establishment of the PDU Session and steps 1 -9 are not performed.

NOTE 1: The definition of the PCO field is for stage 3 to specify.

1. SMF+PGW-C configures an Access Control List (ACL) in UPF+PGW-U to stop any traffic over the default PDN Connection until the UUAA has been done and successful.

2. Steps 14 - 22 in figure 5.3.2.1-1 of TS 23.401 [6] and steps 3 - 6 in figure 4.11.1.5.2-1 of TS 23.502 [3] or clause 4.11.2.4.1 of TS 23.502 [3].

During the Attach procedure, at step 15 of Figure 5.3.2.1-1 in TS 23.401, the SMF+PGW-C includes, in PCO, an Indication to the UE that "UpLink Data NOT ALLOWED" on the PDN connection. The UE shall not send Uplink data to the network, until it receives an indication further from the network that "UpLink Data ALLOWED".

3. UUAA is invoked as described in steps 1 and 2 of figure 5.2.3.2-1.

4. [Conditional] Multiple round-trip messages as required by the authentication method used by USS. This step is performed if the Naf_Authentication_AuthenticateAuthorize response messages from USS in step 4a does not contain a SUCCESS/FAILURE indication. The PCO including the authentication message from the USS is transferred to the UE by the SMF+PGW-C in Update Bearer Request and Downlink NAS Transport (steps 4b - 4d). The response from the UE is transferred to the SMF+PGW-C in an Uplink NAS Transport and Update Bearer Response (steps 4e - 4g).

5. UUAA procedure continues as described in steps 4 & 5 of figure 5.2.3.2-1.

6. If the authentication/authorization is successful, the USS shall subscribe to the PDN Connection Status Event as described in steps 1-5 in figure 4.15.3.2.3-1 of TS 23.502 [3]. This step can be executed in parallel to step 5. The UAS NF/NEF determines the APN/DNN to subscribe to the PDN Connection Status Event notification as specified in clause 5.2.3.1.

7. If the UUAA is successful, the SMF+PGW-C contacts the PCF to update the PDN Connection. Then the SMF+PGW-C updates the Access Control List (ACL) and policies in the UPF+PGW-U to allow traffic over the default PDN Connection. If a DN Authorization Profile Index was received from the UAS NF/NEF SMF+PGW-C in previous step, the SMF+PGW C includes that when retrieving the ACL from the PCF. If the SMF receives the DN authorized Session AMBR in from the UAS NF/NEF, it sends the DN authorized Session AMBR within the Session AMBR to the PCF to retrieve the authorized Session AMBR (described in clause 6.4 of TS 23.503 [9]).

8. The SMF+PGW-C updates the UE by invoking the PDN GW initiated bearer modification without QoS update procedure (figure 5.4.3-1 of TS 23.401 [6]) initiated by sending an Update Bearer Request message to the SGW. The PCO includes an indication that "UpLink Data ALLOWED", the UUAA Aviation Payload i.e. the Authentication/Authorization result and the Authorization Data. The UE (for the UAV) confirms the update (see clause 5.4.3 of TS 23.401 [6]).

9. If the USS in step 6 subscribed to the PDN Connection Status Event the SMF+PGW-C will, as described in steps 6-7 in Figure 4.15.3.2.3-1 of TS 23.502 [3], detect when the PDN Connection is established and send the PDN Connection Establishment event report to the UAS NF/NEF by means of Nsmf_EventExposure_Notify message, including GPSI and the UE IP Address. Then, the UAS NF/NEF forwards the event message to the USS.

5.2.4 UUAA Re-authentication and Re-authorization by USS/UTM

5.2.4.1 UAV Re-authentication procedure in 5GS

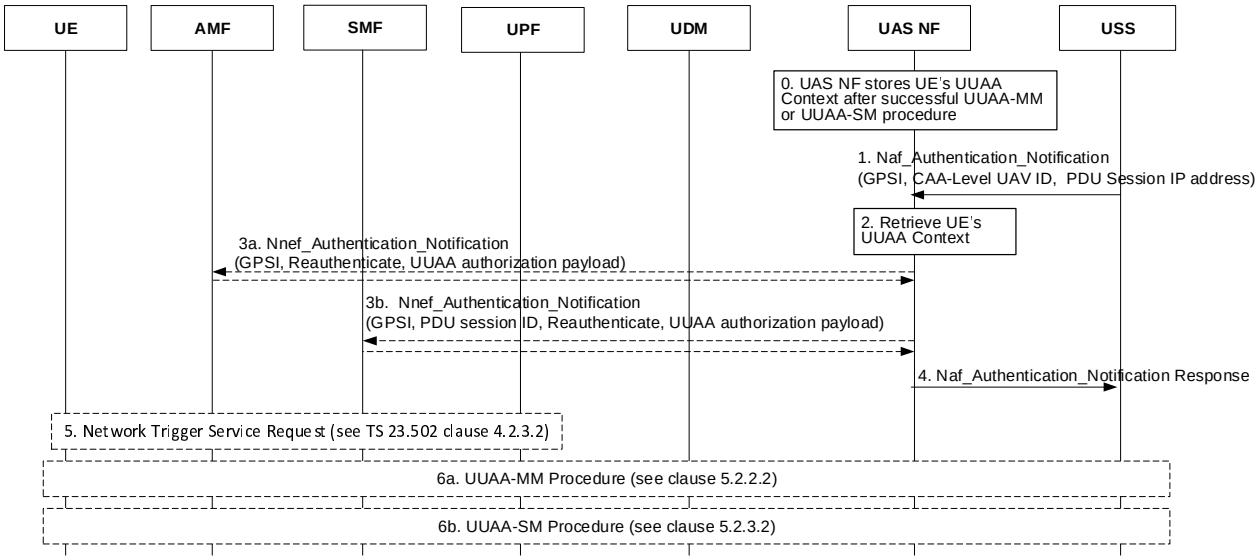

Figure 5.2.4.1-1: UAV Re-authentication procedure in 5GS

UAS NF stores the UE UUAA context after successful UUAA procedure as explained in clause 5.2.2.2 for UUAA-MM and in clause 5.2.3 for UUAA-SM procedure. The UUAA context may be stored in the UDSF or may be stored locally in the UAS NF depending on deployments.

1. The USS sends a Naf_Authentication_Notification request to UAS NF for re-authentication of the UAV. The USS includes GPSI, CAA-Level UAV ID, PDU Session IP address if available in the re-authentication request and an authentication message to be transparently delivered to the UAV.

2. UAS NF retrieves the stored UUAA context for the UE. From the stored UUAA context the UAS NF determines the target AMF or SMF for sending the notification.

3a or 3b. The UAS NF sends Nnef_Authentication_Notification request to notify the target NF, i.e. either the AMF or the SMF, to initiate re-authentication of the UAV.

4. The UAS NF responds back to the USS indicating that re-authentication request has been successfully initiated

5. If UE is in CM_Idle state, the target NF (i.e. either the AMF or the SMF) initiates the Network Triggered Service Request procedures as described in clause 4.2.3.3 of TS 23.502 [3].

6a. If UUAA-MM was performed, the AMF initiates re-authentication of the UAV as described in steps 4c to 10 of UUAA-MM procedure, clause 5.2.2.2.

6b. If UUAA-SM was performed, the SMF then initiates re-authentication of the UAV as described in steps 3c to 7 of the UUAA-SM procedure, clause 5.2.3.2.

5.2.4.2 UAV Re-authentication procedure in EPS

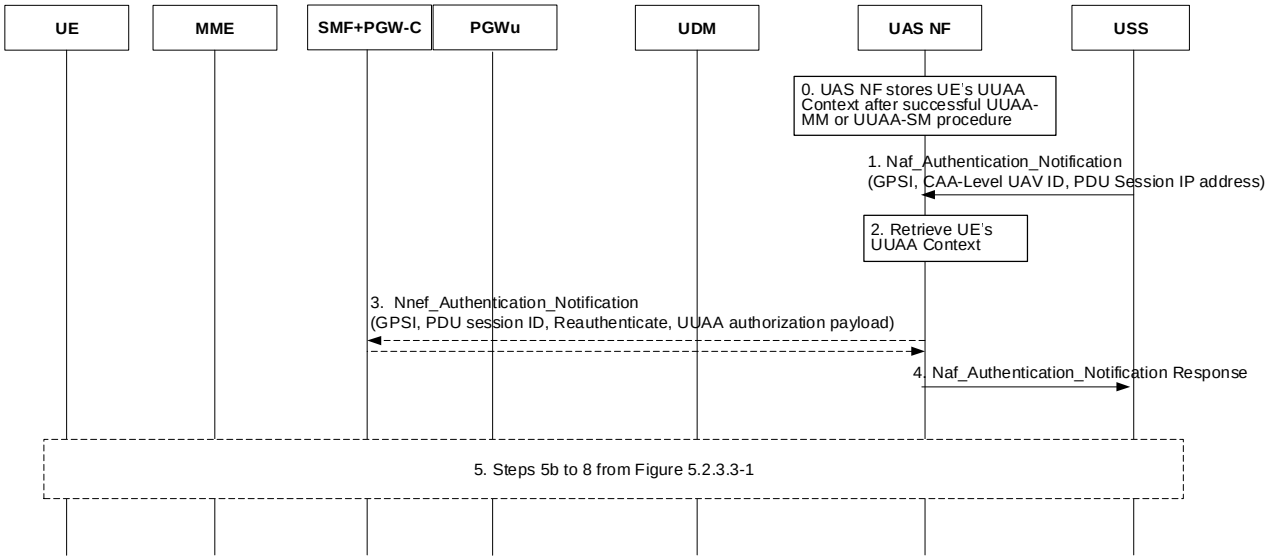

Figure 5.2.4.2-1: UAV Re-authentication procedure in EPS

UAS NF stores the UE UUAA context after successful UUAA-SM procedure as explained in clause 5.2.3. The UUAA context may be stored in the UDSF or may be stored locally in the UAS NF depending on deployments.

1. The USS sends a Naf_Authentication_Notification request to UAS NF for re-authentication of the UAV. The USS includes GPSI, CAA-Level UAV ID, UE IP address in the re-authentication request and an authentication message to be transparently delivered to the UAV.

2. UAS NF retrieves the UE stored UUAA context. From the stored UUAA context the UAS NF determines the target SMF+PGW-C for sending the notification.

3. The UAS NF sends Nnef_Authentication_Notification request to notify the SMF+PGW-C, to initiate re-authentication of the UAV.

4. The UAS NF responds back to the USS indicating that re-authentication request has been successfully initiated

5. The SMF+PGW-C then initiates re-authentication of the UAV as in steps 5b to 8 in Figure 5.2.3.3-1: UUAA during PDN connection establishment at Attach procedure in EPS.

5.2.4.3 USS initiated UAV Re-authorization procedure in 5GS

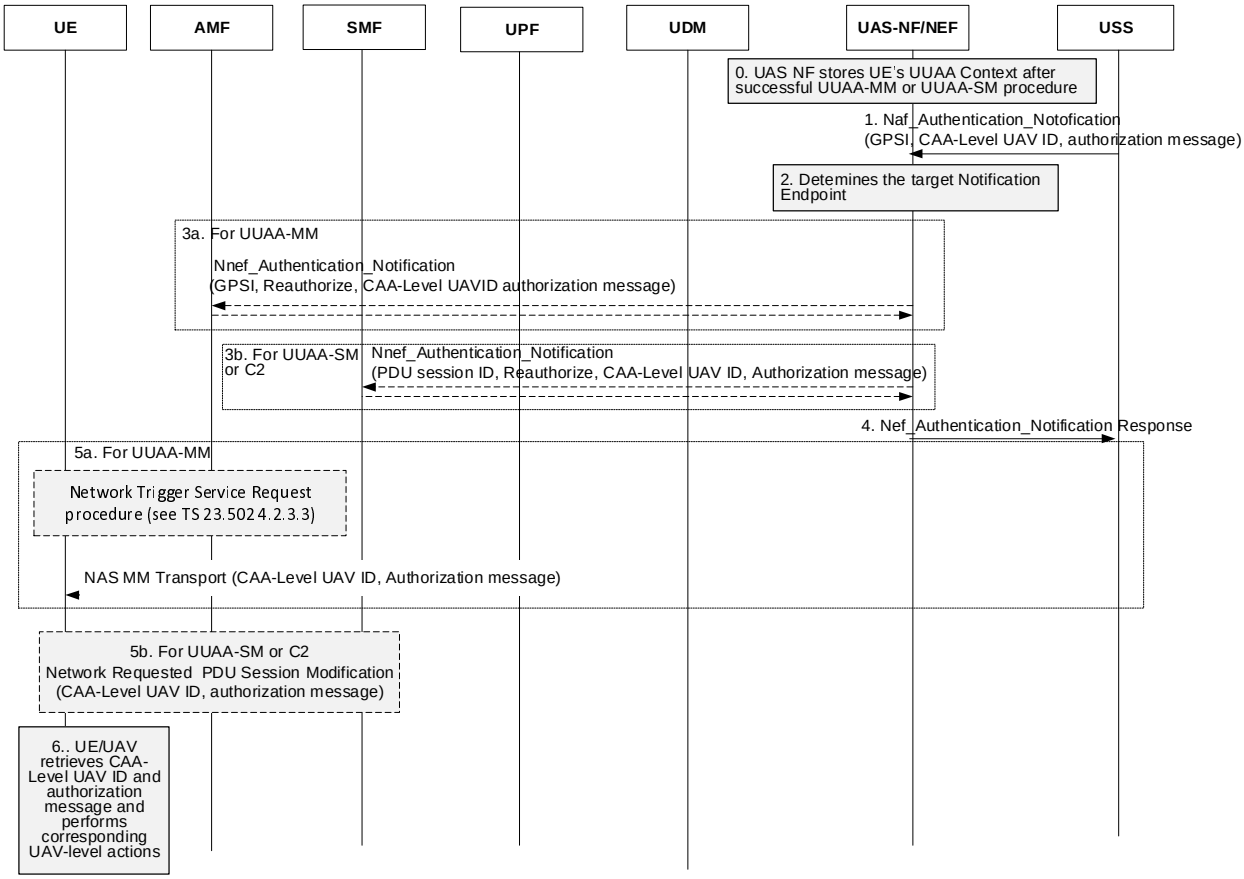

Figure 5.2.4.3-1: UAV Re-authorization procedure in 5GS

UAS NF stores the UE UUAA context after successful UUAA procedure as explained in clause 5.2.2.2 for UUAA-MM and in clause 5.2.3 for UUAA-SM procedure. The UUAA context may be stored in the UDSF or may be stored locally in the UAS NF depending on deployments.

1. The USS sends a Naf_Authentication_Notification request to UAS NF for re-authorization of the UAV. The USS includes GPSI, CAA-Level UAV ID, Notification Correlation Information, an authorization message to be transparently delivered to the UAV. The CAA-Level UAV ID may be a new CAA-Level UAV ID. The authorization message may e.g. include a UUAA Authorization Payload, a C2 Authorization Result and a C2 Authorization Payload (e.g. containing C2 pairing information and C2 security information).

2. Based on the received GPSI and Notification Correlation Information from the USS, the UAS NF/NEF determines the corresponding Notification Correlation Information for Nnef_Authentication_Notification request.

3a For UUAA-MM re-authorization, the UAS-NF/NEF sends a Nnef_Authentication_Notification request including the CAA-Level UAV ID and the authorization message to the serving AMF.

3b For UUAA-SM re-authorization or C2 re-authorization, the UAS-NF/NEF sends a Nnef_Authentication_Notification request to the SMF serving the UUAA or C2 for the UE which includes the corresponding PDU session identity, CAA-Level UAV ID and the authorization message.

4. The UAS NF responds back to the USS indicating that re-authorization request has been successfully initiated.

5a. In the case of UUAA-MM:

If the UE is in CM_Idle state, the AMF initiates the Network Triggered Service Request procedures as described in clause 4.2.3.3 of TS 23.502 [3].

The AMF delivers the CAA-Level UAV ID and the authorization message to the UE using NAS MM Transport.

5b In the case of UUAA-SM or C2 re-authorization:

The SMF identifies, based on the received information, the PDU Session that is serving the UUAA-SM or C2 re-authorization and invokes the Network Requested PDU Session Modification procedure (figure 4.3.3.2-1 of TS 23.502 [3] triggering event SMF Requested modification) by sending Namf_Communication_N1N2MessageTransfer, including the CAA-Level UAV ID and the authorization message in the N1_SM_Container (step 3b in figure 4.3.3.2-1 of TS 23.502 [3]) .

The Network Triggered service request procedure is invoked by AMF to forward the CAA-Level UAV ID and the authorization message included in the N1_SM_container to the UE (from step 3a in figure 4.2.3.3-1 of TS 23.502 [3]).

6. The UE receives the CAA-Level UAV ID and the authorization message, which may e.g. include a UUAA Authorization Payload, a C2 Authorization Result and a C2 Authorization Payload (e.g. containing C2 pairing information and C2 security information). The UE acts on it accordingly (outside the scope of 3GPP).

NOTE: The UAV-C replacement procedure is described in clause 5.2.8. The C2 connectivity revocation procedure is described in clause 5.2.9.

5.2.4.4 USS initiated UAV Re-authorization procedure in EPS

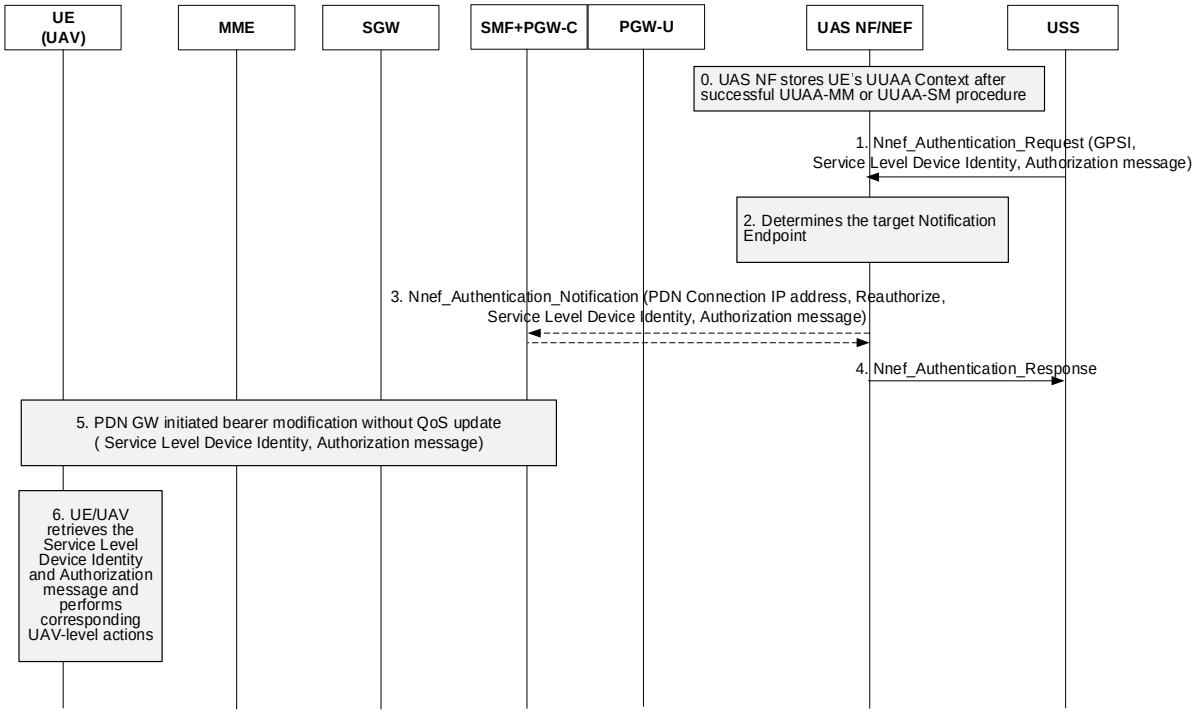

Figure 5.2.4.4-1: UAV Re-authorization procedure in EPS

UAS NF/NEF stores the UE UUAA context after successful UUAA procedure as in clause 5.2.3 for UUAA-SM procedure. The UUAA context may be stored in the UDSF or may be stored locally in the UAS NF/NEF depending on deployments.

1. The USS sends a request to UAS NF/NEF for re-authorization of the UAV. The USS includes GPSI, Service Level Device Identity (e.g. CAA-Level UAV ID), Notification Correlation Information and authorization message to be transparently delivered to the UAV. The Service Level Device Identity (e.g. CAA-Level UAV ID) may be a new Service Level Device Identity (e.g. CAA-Level UAV ID). The authorization message may e.g. include a UUAA Authorization Payload, a C2 authorization result and a C2 Authorization Payload (e.g. containing, C2 pairing information and C2 security information).

2. Based on the received GPSI and Notification Correlation Information from the USS, the UAS NF/NEF determines the corresponding Notification Correlation Information for Nnef_Authentication_Notification request.

NOTE 1: In EPS the UUAA context is always UUAA-SM.

3. The UAS NF/NEF sends a Nnef_Authentication_Notification request to the SMF+PGW-C serving the UUAA or C2 which includes the corresponding PDN Connection identity, Service Level Device Identity (e.g. CAA-Level UAV ID) and the authorization message.

4. The UAS NF/NEF responds back to the USS indicating that re-authorization request has been successfully initiated.

5. The SMF+PGW-C identifies, based on the received information, the PDN Connection that is serving the UUAA-SM and invokes the PDN GW initiated bearer modification without QoS update procedure (figure 5.4.3-1 of TS 23.401 [6]) by sending Update Bearer Request message, including the Service Level Device Identity (e.g. CAA-Level UAV ID) and the authorization message in the PCO.

   The Update Bearer Request message including the Service Level Device Identity (e.g. CAA-Level UAV ID) and the authorization message is forwarded by MME as Downlink NAS Transport to the UE (steps 4 and 5 in figure 5.4.3-1 of TS 23.401 [6]).

6. The UE receives the Service Level Device Identity (e.g. CAA-Level UAV ID) and the authorization message (which may e.g. include a UUAA Authorization Payload, a C2 authorization result and a C2 Authorization Payload (e.g. containing C2 pairing information and C2 security information). The UE acts on it accordingly (outside scope of 3GPP).

NOTE 2: The UAV-C replacement procedure is described in clause 5.2.8. The C2 connectivity revocation procedure is described in clause 5.2.9.

5.2.5 Authorization for C2

5.2.5.1 General

Authorization for C2 is required when a UAV establishes a user plane connection for C2 operations, i.e. to deliver messages with information of command and control for UAV operations from a UAV-C or USS to a UAV or to report telemetry data from a UAV to its UAV-C. Two sides of C2 communication, i.e. UAV and UAV-C, belong to the same UAS.

A UAV shall be authorized by the USS to use a PDU Session/PDN connection for C2. Authorization for C2 includes the following:

- UAV to UAV-C pairing authorization: Authorization for pairing with a networked UAV-C or a UAV-C that connects to the UAV via Internet connectivity, before the UAV and the UAV-C can exchange C2 communication. One UAV can be paired with only one UAV-C at the any time. One UAV-C may be paired with one or more UAVs at the same time.

- Flight Authorization: Authorization for flight when UAV also provides Flight Authorization information.

C2 authorization may be carried out:

- During the UUAA procedure (if UUAA is carried out at PDU session/PDN connection establishment) as described in clause 5.2.3 when the UAV requests establishment of PDU Session/PDN connection for connectivity.

- During PDU Session Modification/ UE requested bearer resource modification when the UAV requires to use an existing PDU session/PDN connection to exchange C2 communication related messages.

- During a new PDU Session/PDN connection establishment, if the UAV requires to use a separate PDU Session/PDN connection for C2 communication.

5.2.5.2 Procedure for C2 authorization in 5GS

5.2.5.2.1 C2 Authorization request during UUAA-SM procedure in 5GS

If C2 authorization is requested during the UUAA-SM procedure the procedure described in clause 5.2.3.2 takes place with the following additions:

- In Step 0, the UE includes pairing information (if available) in a C2 Aviation Payload. which is forwarded further to the USS;

- In step 4, the USS performs C2 authorization taking into account the included pairing information, the Service Level Device Identity/CAA-Level UAV ID and 3GPP UAV ID/GPSI. The USS includes the resulting C2 Authorization result and optionally a C2 authorization payload in the Naf_Authentication_AuthenticateAuthorize response returned to the UAS-NF/NEF and the UAS NF/NEF forwards to the UAV/UE in step 7.

- The USS shall:

  - in step 4 include a DN Authorization profile Index specifying a predefined set of PCC-rules in the PCF with initial restriction on the type of traffic allowed to pass on the PDU-session. For example, only traffic exchanged with the USS might be allowed to pass.

    Once the authentication is complete, after step 4, the USS subscribes to PDU Session Status Events for the PDU session used for C2 communication, applicable for the GPSI received in step 2.

  - when the USS in step 8 receives a PDU Session State Event Report indicating session start and including the PDU Session IP address the USS invokes the USS initiated pairing policy configuration procedure (see figure 5.2.5.4.1-1) with the received PDU Session IP address and authorized paired UAV-C IP-address as input to request corresponding traffic to be allowed on the PDU session in the UPF.

5.2.5.2.2 UE initiated PDU Session Modification for C2 Communication

C2 authorization is requested at PDU session Modification:

- After UUAA-SM is performed and a common PDU session is used for connectivity to USS and C2 communication to a UAV-C (as configured in the UAV); or

- If the UE has already established a PDU session for C2 communication to a UAV-C.

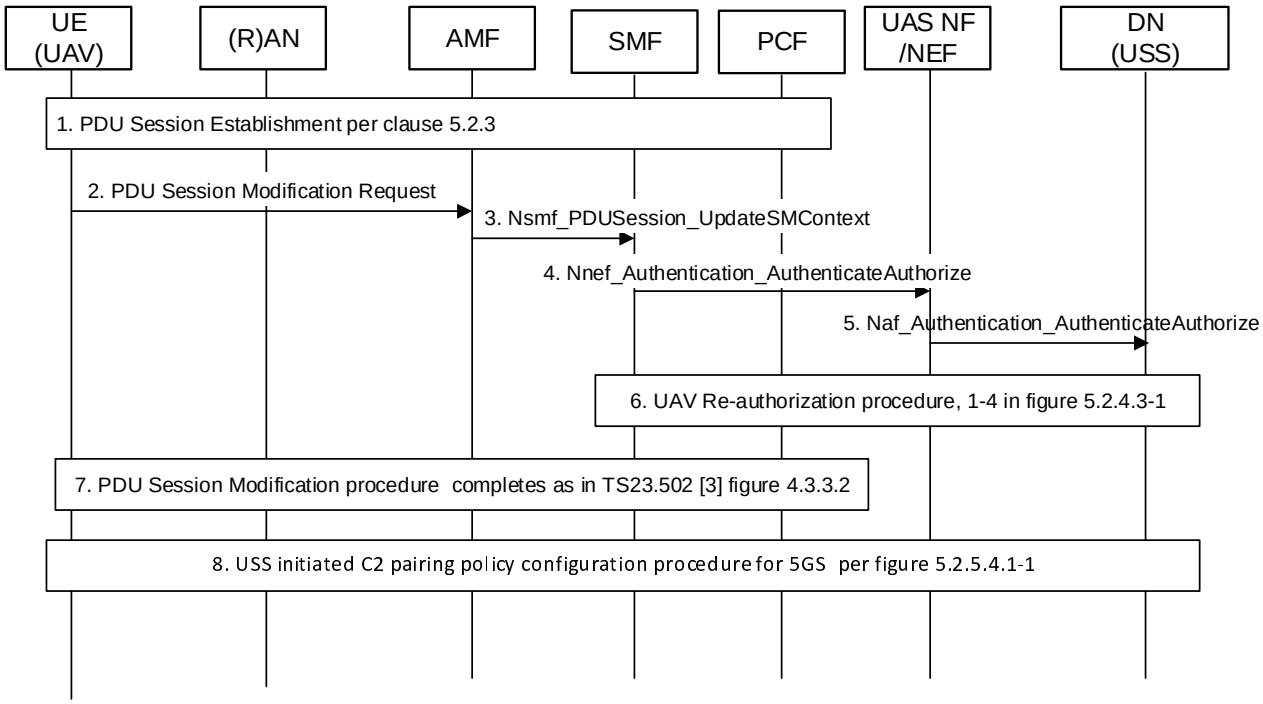

Figure 5.2.5.2.2-1: PDU Session modification for C2 communication (common PDU session for UAS services)

1. The UE establishes a PDU Session for USS communication as described in clause 5.2.3.

2-3. When the UAV needs to establish C2 communication the UAV determines that an existing PDU session can be used and initiates a PDU Session Modification procedure. The UE shall include in the request a CAA-Level UAV ID and shall include a C2 Aviation Payload within a UAS container that includes C2 authorization

information. The USS may also use its locally configured pairing information for UAV - UAV-C pairing authorization which takes precedence over UAV provided pairing information. The pairing information includes the CAA-level UAV ID of the requesting UE and also includes identification information of UAV-C to pair if available. The UAV may also include other information such as Flight Authorization information.

NOTE: How the pairing information is configured in the UAV is outside the scope of 3GPP specifications.

4. The SMF determines that authorization is required based on that the DNN/S-NSSAI of the PDU session is dedicated for aerial services (have aerial service indicator set) and that the Service Level Device Identity (CAA-Level UAV ID) is included in the request and Then sends a Nnef_Authentication_AuthenticateAuthorize request to the UAS-NF including the UAS container provided by the UAV in step 2 (including the C2 Aviation Payload), the CAA-Level UAV ID, GPSI, PDU Session IP address, and optionally the UAV location (e.g. Cell ID) provided by the AMF.

5. The UAS-NF forwards the received authorization request as a Naf_Authentication_AuthenticateAuthorize request to the USS.

6. Triggered by step 5, the USS performs C2 authorization based on the received information and invokes, in order to forward the C2 authorization result to the UAV/UE, the UAV Re-authorization procedure (see figure 5.2.4.3-1) including GPSI, CAA-Level UAV-ID (potentially new) and included in the authorization message, the C2 Authorization Result and the C2 Authorization Payload (e.g. containing C2 pairing information and C2 security information).

7. PDU Session Modification procedure forwards the C2 authorization result to the UAV/UE and completes as in figure 4.3.3.2-1 of TS 23.502 [3].

8. The USS invokes, with the received PDU Session IP address and the IP address of the authorized paired UAV-C as input, the USS initiated pairing policy configuration procedure (see figure 5.2.5.2.4-1) to request corresponding traffic to be allowed on the PDU session in the UPF.

Unless a dedicated QoS is requested for the C2 flows, this procedure does not invoke any interaction with the UE, AMF or RAN.

5.2.5.2.3 UE initiated PDU Session Establishment for C2 Communication

If C2 authorization is requested during PDU session establishment to a PDU session used specifically for C2 communication to UAV-C the UAV requests C2 authorization as follows.

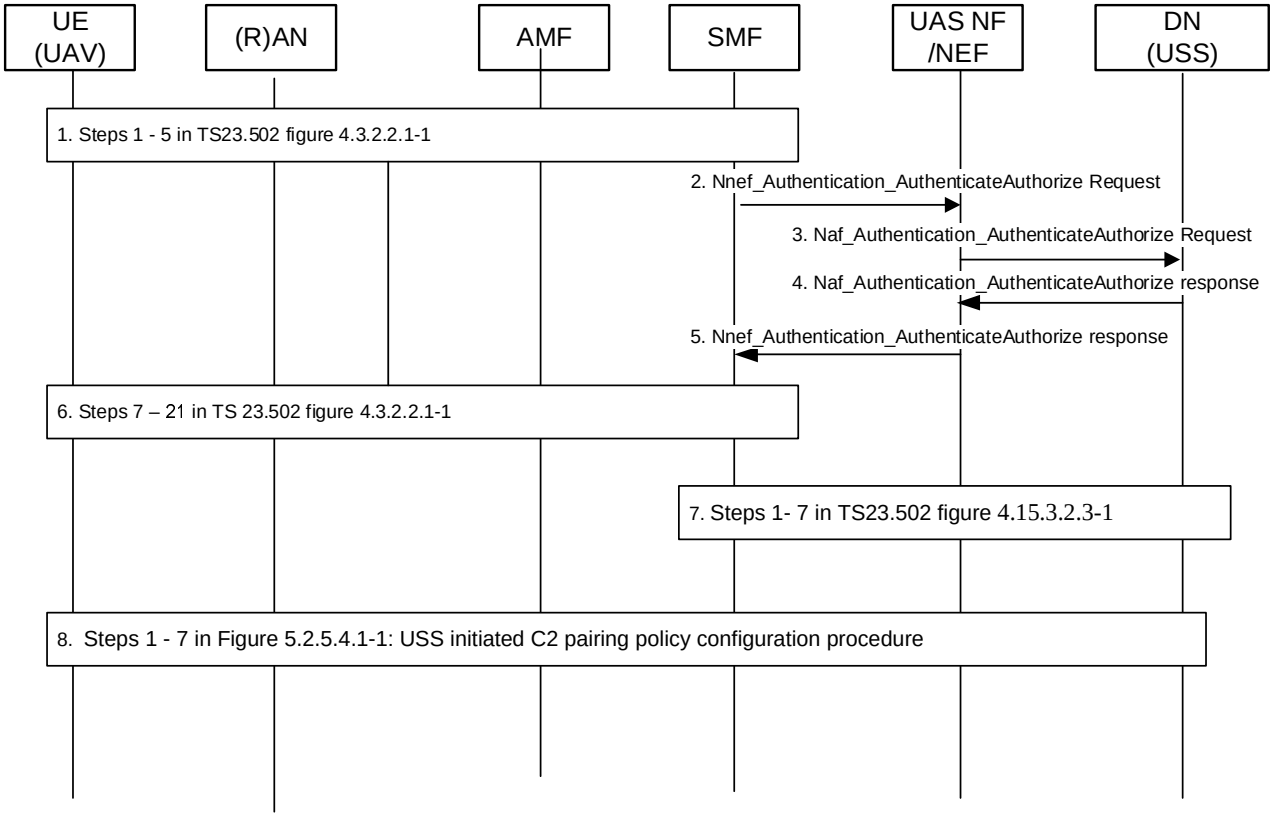

Figure 5.2.5.2.3-1: PDU Session establishment for C2 communication (separate PDU Sessions for UAS services)

0. The UAV has performed a successful UUAA with the USS (UUAA-SM or UUAA-MM) and the USS has for the corresponding GPSI subscribed for PDU Session Status Event from the NEF.

1. When the UAV needs to establish C2 communication the UAV determines that a new dedicated PDU session is required for connectivity to UAV-C. The UE initiates PDU Session establishment procedure for a DNN/S-NSSAI dedicated for connectivity to UAV-C. In the PDU Session establishment request CAA-Level UAV ID and a C2 Aviation Payload to be used for C2 authorization shall be included and forwarded to the SMF. The pairing information includes the CAA-Level UAV IDs of the requesting UAV and identification information for the UAV-C to pair may be included in C2 Aviation Payload. The UAV may also include other information such as Flight Authorization information. The USS may also use its locally configured pairing information for UAV - UAV-C pairing authorization which then takes precedence over UAV provided pairing information.

2. The SMF determines that authorization is required based on that the requested DNN/S-NSSAI combination dedicated for aerial services (have aerial service indicator set), and that the Service Level Device Identity (CAA-Level UAV ID) is included in the request. The SMF then sends a Nnef_Authentication_AuthenticateAuthorize request, which is used to request authorization to pair the UAV with UAV-C, to the UAS NF/NEF that includes the GPSI, CAA-Level UAV ID and C2 Aviation Payload and optionally the UAV location (e.g. Cell ID) if provided by the AMF and the DNN and S-NSSAI of the PDU session.

   If the requested DNN/S-NSSAI is dedicated for aerial services but no Service Level Device ID (CAA-Level UAV ID) has been provided with the request, the SMF rejects the PDU session establishment with a cause indicating that USS authorization is required.

   The SMF also provides a Notification Endpoint to the UAS NF/NEF. By providing the Notification Endpoint, the SMF is implicitly subscribed to be notified of re-authorization, update authorization data or revocation of C2 connectivity from UAS NF/NEF, if the C2 authorization result is successful in step 5.

3. The UAS NF/NEF checks that a valid UUAA is stored for the GPSI and forwards the received authorization request as a Naf_Authentication_AuthenticateAuthorize request to the USS. If not, the request is not forwarded to the USS and the PDU session is rejected.

The UAS NF/NEF also provides a Notification Endpoint to the USS. By providing the Notification Endpoint, the UAS NF/NEF is implicitly subscribed to be notified of re-authorization, update authorization data or revocation of C2 connectivity from USS, if the UUAA result is successful in step 5.

NOTE: The USS may trigger a UAV re-authentication/re-authorization in response to the query from the UAS NF/NEF.

4. The USS performs C2 authorization based on the received information and sends the Naf_Authentication_AuthenticateAuthorize response to the UAS NF/NEF including the Service Level Device Identity (e.g. the CAA-Level UAV-ID) (potentially new), the C2 Authorization Result and the C2 Authorization Payload (e.g. C2 pairing information and C2 security information).

5. The UAS-NF/NEF forwards the information received from the USS in the Nnef_Authentication_AuthenticateAuthorize response sent to the SMF.

6. To inform the UE about the C2 Authorization Result the SMF includes the authorization result and, optionally, a new CAA-Level UAV ID if received from the USS, in the PDU Session Accept sent to the UE and let the PDU session establishment procedure continue until finalized.

   If a failed C2 Authorization Result is received from the USS, the SMF instead rejects the PDU establishment and include a reason code indicating not authorized.

7. [Conditional] If the C2 authorization is successful the USS subscribes via the UAS-NF to a PDU Session Status event for the PDU session used for C2 including in the request the GPSI of the UAV. The UAS NF determines DNN, S-NSSAI corresponding to the PDU session used for C2 communication and uses this DNN, S-NSSAI to subscribe to SMF for PDU Session Status event. The SMF detects, as described in step 6-7 of figure 4.15.3.2.3-1 in TS 23.502 [3], when the PDU Session is established and send the PDU Session Status event report to the UAS NF/NEF by means of Nsmf_EventExposure_Notify message, including GPSI and UE IP Address. The UAS NF/NEF then forwards the event message to the USS.

8. [Conditional] The USS stores the received UE IP address and invokes, with the received PDU Session IP address and the IP-address of the authorized paired UAV-C as input, the USS initiated pairing policy configuration procedure (see figure 5.2.5.2.4-1) to request corresponding traffic to be allowed on the PDU session by the UPF.

   Unless a dedicated QoS is requested for the C2 flows, this procedure does not invoke any interaction with the UE, AMF or RAN.

5.2.5.3 Procedure for C2 authorization in EPS

5.2.5.3.0 C2 Authorization request during UUAA-SM procedure in EPS

If C2 authorization is requested during the UUAA-SM procedure the procedure described in clause 5.2.3.3 takes place with the following additions:

- In step 0, the UE includes pairing information (if available) in a C2 Aviation Payload, which is forwarded further to the USS.

- Initially in step 5, the USS performs C2 authorization taking into account the included pairing information, the Service Level Device Identity/CAA-Level UAV ID and 3GPP UAV ID/GPSI. The USS includes the resulting C2 Authorization result in the Naf_Authentication_AuthenticateAuthorize response returned to the UAS-NF/NEF and UAS NF/NEF forwards to the UAV/UE in step 8.

- The USS shall:

  - in step 5 include a DN Authorization profile Index specifying a predefined set of PCC-rules in the PCF with initial restriction on the type of traffic allowed to pass on the PDN Connection. For example, only traffic exchanged with the USS might be allowed to pass.

    Once the authentication is complete, after step 5, the USS subscribes to PDN Connectivity Status Events for the PDN Connection used for C2 communication, applicable for the GPSI received in step 2.

  - when the USS in step 9 receives a PDN Connectivity Status Event Report indicating session start and including the PDN Connection IP address, the USS invokes the USS initiated pairing policy configuration

procedure (see figure 5.2.5.4.2-1) with the received PDN Connection IP address and authorized paired UAV-C IP-address as input to request corresponding traffic to be allowed on the PDN Connection in the PGW-U.

5.2.5.3.1 UE requested PDN connectivity for C2 authorization

When the UAV requests to establish connectivity to an additional PDN over E-UTRAN for C2, the procedure described in clause 5.10.2 of TS 23.401 [6] takes place with the following modifications:

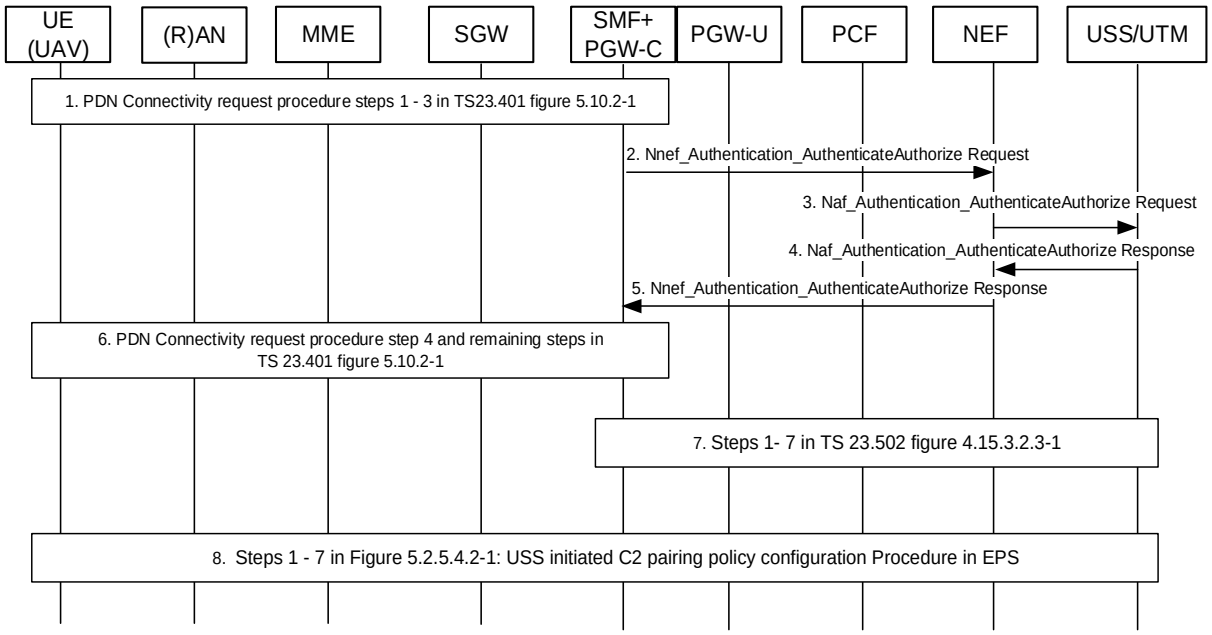

Figure 5.2.5.3.1-1: UE requested PDN Connectivity for C2 authorization

0. The UAV has performed a successful UUAA with the USS (UUAA-SM) and the USS has for the corresponding GPSI subscribed for PDN Connectivity Status Event reports from the NEF.

1. Steps 1 - 3 performed as in Figure 5.10.2-1 of TS 23.401 [6].

   When the UAV needs to establish C2 communication, the UAV determines that a new PDN Connection is required for connectivity to UAV-C. The UE initiates a UE Requested PDN Connectivity procedure for connectivity to UAV-C. In the PCO in the PDN Connectivity Request, the Service Level Device Identity (e.g. the CAA-Level UAV ID) and a C2 Aviation Payload to be used for C2 authorization shall be included and forwarded to the MME. The pairing information includes the Service Level Device Identity (e.g. CAA-Level UAV IDs) of the requesting UAV and identification information for the UAV-C to pair may be included in C2 Aviation Payload. The UAV may also include other information such as Flight Authorization information. The USS may also use its locally configured pairing information for UAV - UAV-C pairing authorization which then takes precedence over UAV provided pairing information.

   If Service Level Device Identity (CAA-Level UAV ID) is provided with the request, the SMF+PGW-C retrieves (if not already available) the Session Management Subscription Data for the UE from the UDM+HSS using the Nudm_SDM_Get service operation.

2. The SMF+PGW-C determines that authorization is required based on that the requested APN/DNN is dedicated for aerial services (have aerial service indicator set) and that the Service Level Device Identity (CAA-Level UAV ID) is included in the request. The SMF+PGW-C then sends a Nnef_Authentication_AuthenticateAuthorize request, which is used to request authorization to pair the UAV with UAV-C, to the UAS NF/NEF that includes the GPSI, Service Level Device Identity (e.g. the CAA-Level UAV ID) and C2 Aviation Payload and optionally the UAV location (e.g. Cell ID) if provided by the MME and the APN/DNN of the PDN Connection.

If the SMF+PGW-C determines that the authorization procedure with the USS is required, but the UAV has not provided the Service Level Device Identity (e.g. the CAA-Level UAV ID), the SMF+PGW-C rejects the PDN Connectivity Request with a cause indicating that USS authorization is required.

3. The UAS NF/NEF checks that a valid UUAA is stored for the GPSI and forwards the received authorization request as a Naf_Authentication_AuthenticateAuthorize request to the USS. If not, the request is not forwarded to the USS and the PDN connection is rejected.

4. The USS performs C2 authorization based on the received information and sends the Naf_Authentication_AuthenticateAuthorize response to the UAS NF/NEF including the Service Level Device Identity (e.g. the CAA-Level UAV-ID) (potentially new), the C2 Authorization Result and the C2 Authorization Payload (e.g. C2 pairing information and C2 security information).

5. The UAS NF/NEF forwards the information received from the USS in the Nnef_Authentication_AuthenticateAuthorize response sent to the SMF+PGW C.

6. To inform the UE about the C2 authorization result the SMF+PGW-C includes the C2 Authorization Result and optionally, the Authorization Payload (e.g. C2 pairing information and C2 security information) and a new Service Level Device Identity (e.g. CAA-Level UAV ID) if received from the USS, in the PCO in the PDN Connectivity Accept sent to the UE and let the PDN Connectivity Request procedure continue until finalized.

   If a failed C2 authorization result is received from the USS, the SMF+PGW-C instead rejects the PDN Connectivity Request and includes a cause code indicating not authorized.

7. If the C2 authorization is successful the USS subscribes via the UAS NF/NEF to a PDN Connection Status Event report for the PDN Connection used for C2 including in the request the GPSI of the UAV. The UAS NF/NEF determines the APN/DNN and uses this APN/DNN to subscribe to SMF+PGW-C for PDN Connection Status Event. The SMF+PGW-C detects, as described in step 6-7 of figure 4.15.3.2.3-1 in TS 23.502 [3], when the PDN Connection is established and sends the PDN Connection Status Event report to the UAS NF/NEF by means of Nsmf_EventExposure_Notify message, including GPSI and UE IP Address. The UAS NF/NEF then forwards the event message to the USS.

8. The USS stores the received UE IP address and invokes, with the received PDN Connection IP address and the IP-address of the authorized paired UAV-C as input, the USS initiated C2 pairing policy configuration in EPS procedure (see figure 5.2.5.4.2-1) to request corresponding traffic to be allowed on the PDN Connection by the PGW-U.

   Unless a dedicated QoS is requested for the C2 flows, this procedure does not invoke any interaction with the UE, MME or RAN.

5.2.5.3.2 UE requested bearer resource modification of an existing PDN connection for C2 authorization

C2 authorization is requested at UE requested bearer resource modification (see clause 5.4.5 of TS 23.401 [6]):

- After UUAA-SM is performed and a common PDN Connection is used for connectivity to USS and C2 communication to a UAV-C (as configured in the UAV); or

- If the UE has already established a PDN Connection for C2 communication to a UAV-C.

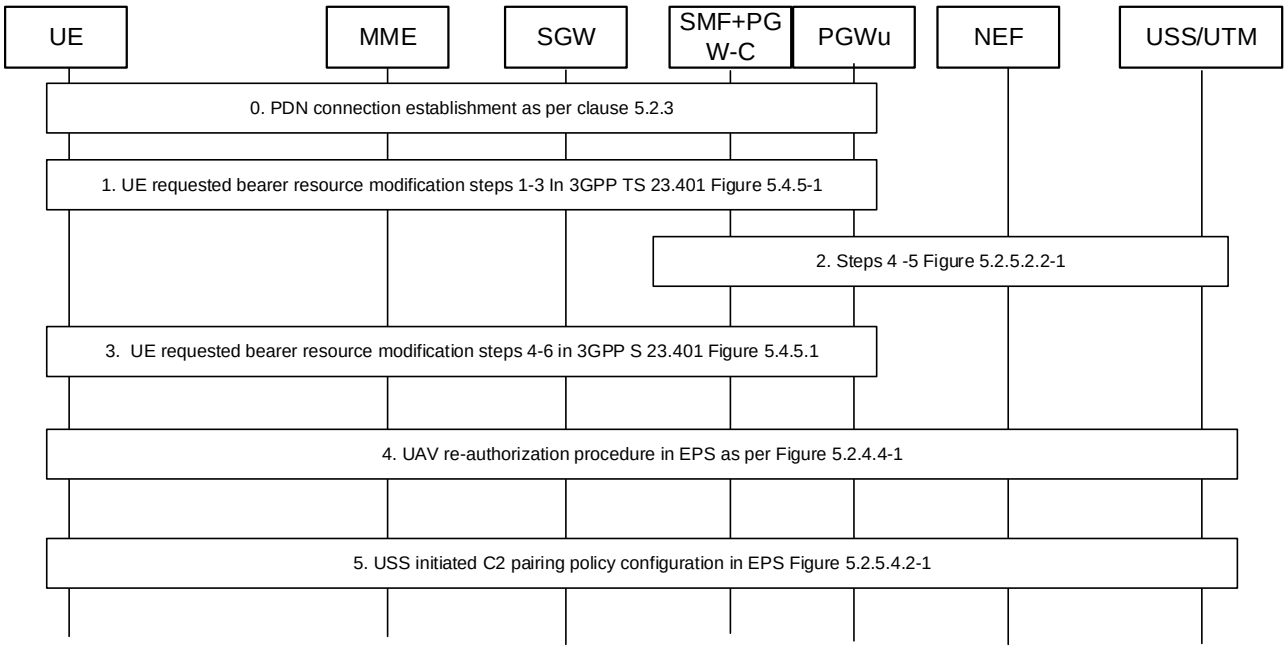

Figure 5.2.5.3.2-1: UE requested bearer resource modification of an existing PDN connection for C2 authorization

0. The UE establishes a PDN Connection for USS communication as described in clause 5.2.3.

1. When the UAV needs to establish C2 communication, the UAV determines that an existing PDN Connection can be used and initiates a UE requested bearer resource modification procedure as Steps 1 - 3 in Figure 5.4.5-1 of TS 23.401 [6]. In the PCO in the request, the UE includes a Service Level Device Identity (e.g. CAA-Level UAV ID) and shall include a C2 Aviation Payload that includes C2 authorization information. The USS may also use its locally configured pairing information for UAV - UAV-C pairing authorization which takes precedence over UAV provided pairing information. The pairing information includes the Service Level Device Identity (e.g. CAA-level UAV ID) of the requesting UE and also includes identification information of UAV-C to pair if available. The UAV may also include other information such as Flight Authorization information.

NOTE: How the pairing information is configured in the UAV is outside the scope of 3GPP specifications.

2. The SMF+PGW-C determines that authorization is required based on that the APN/DNN of the PDN Connection is dedicated for aerial services (have aerial service indicator set) and that the Service Level Device Identity (CAA-Level UAV ID) is included in the request and then sends a Nnef_Authentication_AuthenticateAuthorize request to the UAS-NF including the UAS information provided by the UAV in step 1 (including the C2 Aviation Payload), the Service Level Device Identity (e.g. CAA-Level UAV ID), GPSI, PDN Connection IP address, and optionally the UAV location (e.g. Cell ID) provided by the MME.

   The UAS-NF forwards the received authorization request as a Naf_Authentication_AuthenticateAuthorize request to the USS.

3. The UE requested bearer resource modification procedure completes as in clause 5.4.5-1 of TS 23.401 [6].

4. Triggered by step 5, the USS performs C2 authorization based on the received information and invokes, in order to forward the C2 authorization result to the UAV/UE, the UAV Re-authorization procedure (see figure 5.2.4.4-1) including GPSI, Service Level Device Identity (e.g. CAA-Level UAV-ID) (potentially new) and, included in the authorization message, the C2 Authorization Result and the C2 Authorization Payload (e.g. containing C2 pairing information and C2 security information).

5. The USS invokes, with the received PDN Connection IP address and the IP address of the authorized paired UAV-C as input, the USS initiated pairing policy configuration procedure (see figure 5.2.5.4.2-1) to request corresponding traffic to be allowed on the PDN Connection in the UPF/PGW-U.

   Unless a dedicated QoS is requested for the C2 flows, this procedure does not invoke any interaction with the UE, MME or RAN.

5.2.5.4 USS initiated C2 pairing policy configuration

5.2.5.4.1 USS initiated C2 pairing policy configuration in 5GS

The USS initiated C2 pairing policy configuration Figure 5.2.5.4.1-1.

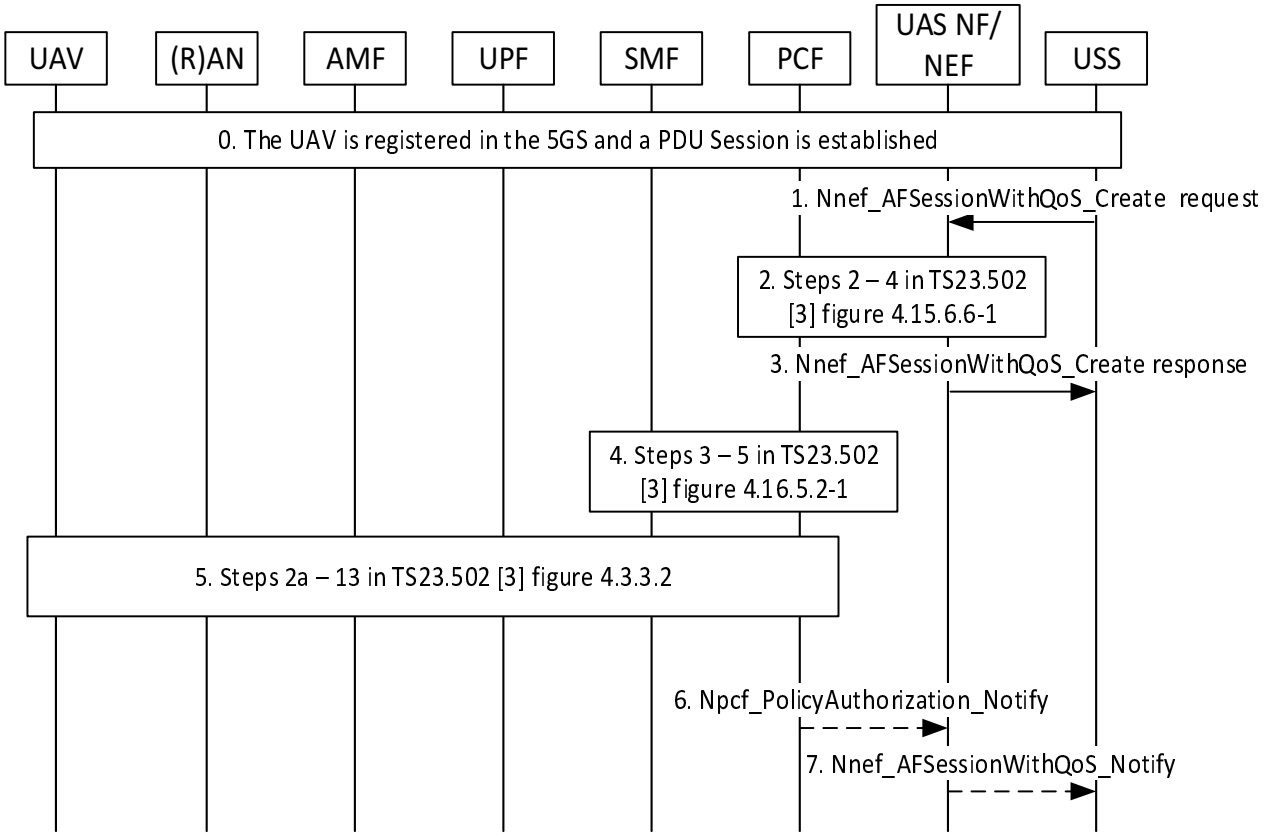

Figure 5.2.5.4.1-1: USS initiated C2 pairing policy configuration in 5GS

0. The UAV is registered in the network and a PDU session is established as specified in clause 5.2.3.2.

1. The USS initiates the PDU Session modification by invoking the Nnef_AFSessionWithQoS_Create request including USS Identity/AF Identifier, UAV-UAVC Pairing info/Flow description(s), QoS reference. The UAV-UAVC Pairing info/Flow description(s) includes the UAV-C IP address. See step 1 in clause 4.15.6.6 of TS 23.502 [3]: Setting up an AF session with required QoS.

2. UAS NF/NEF authorizes the request from the USS followed by interacting with PCF triggering a Npcf_PolicyAuthorization_Create request and provides relevant parameters to the PCF.

   PCF determines whether the request is authorized and if the requested QoS is allowed. PCF informs UAS NF/NEF if the request is accepted by invoking Npcf_PolicyAuthorization_Create response. See steps 2 - 4 in figure 4.15.6.6.6-1 of TS 23.502 [3].

3. UAS NF/NEF sends a Nnef_AFsessionWithQoS_Create response message (Transaction Reference ID, Result) to the USS. Result indicates whether the request is granted or not. See step 5 in figure 4.15.6.6.6-1 of TS 23.502 [3].

NOTE: Use of Nnef_AFSessionWithQoS_Create can be further evaluated with stage 3 work.

4. If the PCF determines that the SMF needs updated policy information, the PCF issues a Npcf_SMPolicyControl_UpdateNotify request with updated policy information. The updated policy information includes the UAV-C IP address. See steps 3 - 5 in figure 4.16.5.2-1 of TS 23.502 [3].

5. The PDU Session Modification continues and completes as in steps 2a - 13 in figure 4.3.3.2-1 of TS 23.502 [3], UE or network requested PDU Session Modification (for non-roaming and roaming with local breakout). Based

on the updated policy information received, the SMF determines and provides N4 rules to enable communication between UAV and UAV-C, e.g. Packet Detection Rules, Forwarding Action Rules.

6-7. [Optional] The PCF sends Npcf_PolicyAuthorization_Notify message to the UAS NF/NEF when the modification of the transmission resources corresponding to the QoS update succeeded or failed. The UAS NF/NEF transfers this information to the USS by sending Nnef_AFSessionWithQoS_Notify message. See steps 6 and 7 in figure 4.15.6.6-1 of TS 23.502 [3].

5.2.5.4.2 USS initiated C2 pairing policy configuration in EPS

The USS initiated C2 pairing policy configuration in EPS figure 5.2.5.4.2-1.

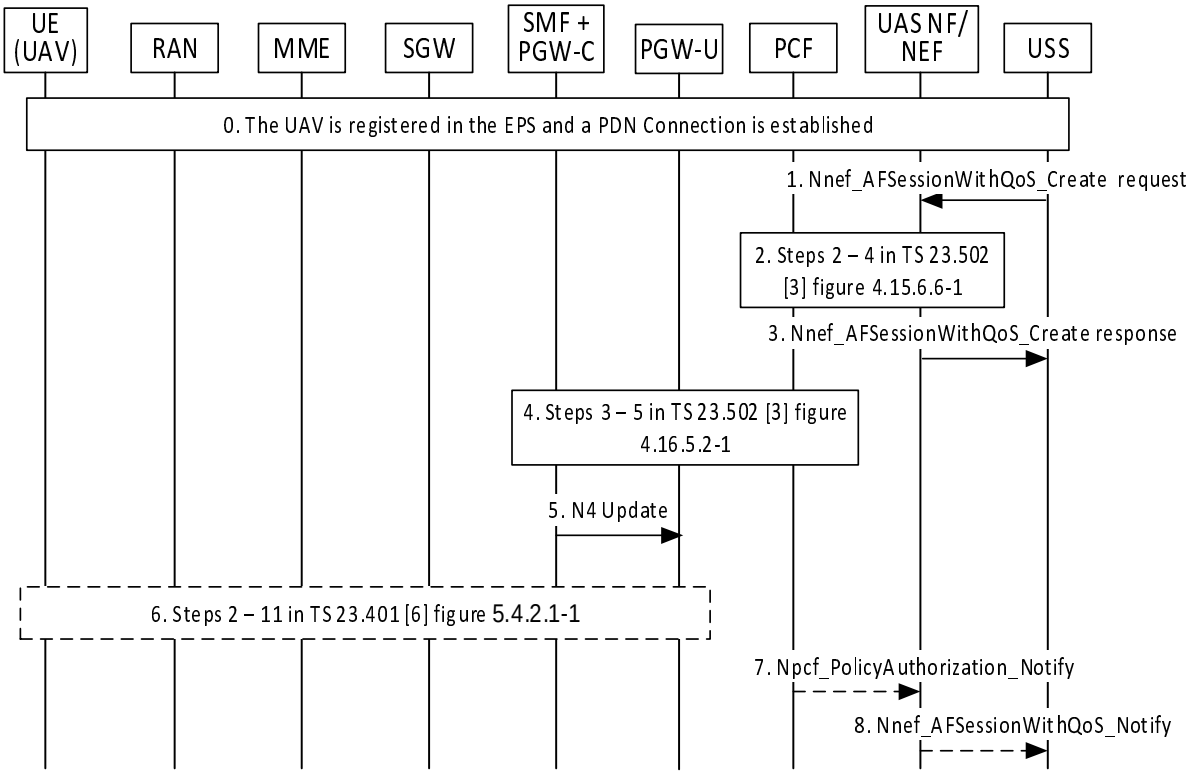

Figure 5.2.5.4.2-1: USS initiated C2 pairing policy configuration in EPS

0. The UAV is registered in the network and a PDN Connection is established as specified in clause 5.2.3.3.

1. The USS initiates the PDN Connection modification by invoking the Nnef_AFSessionWithQoS_Create request including USS Identity/AF Identifier, Transaction Reference ID, UAV-UAVC Pairing info/Flow description(s), QoS reference. The UAV-UAVC Pairing info/Flow description(s) includes the UAV-C IP address. See step 1 in clause 4.15.6.6 of TS 23.502 [3]: Setting up an AF session with required QoS.

2. UAS NF/NEF authorizes the request from the USS followed by interacting with PCF triggering a Npcf_PolicyAuthorization_Create request and provides relevant parameters to the PCF.

   PCF determines whether the request is authorized and if the requested QoS is allowed. PCF informs UAS NF/NEF if the request is accepted by invoking Npcf_PolicyAuthorization_Create response. See steps 2 - 4 in figure 4.15.6.6.6-1 of TS 23.502 [3].

3. UAS NF/NEF sends a Nnef_AFsessionWithQoS_Create response message (Transaction Reference ID, Result) to the USS. Result indicates whether the request is granted or not. See step 5 in figure 4.15.6.6.6-1 of TS 23.502 [3].

NOTE: Use of Nnef_AFSessionWithQoS_Create can be further evaluated with stage 3 work.

4. If the PCF determines that the SMF+PGW-C needs updated policy information, the PCF issues a Npcf_SMPolicyControl_UpdateNotify request with updated policy information. The updated policy information includes the UAV-C IP address. See steps 3 - 5 in figure 4.16.5.2-1 of TS 23.502 [3].

5. Based on the updated policy information received, the SMF+PGW-C determines and provides N4 rules to enable communication between UAV and UAV-C, e.g. Packet Detection Rules, Forwarding Action Rules.

6. [Conditional] If QoS needs to be updated: Based on the updated policy information received, the SMF+PGW-C determines N4 rules for QoS update and provides to the PGW-U.

Based on the updated policy information received, the SMF+PGW-C invokes the PDN GW initiated bearer modification with bearer QoS update procedure (clause 5.4.2.1 in TS 23.401 [6]) by sending Update Bearer Request message to the SGW. Steps 2 - 11 in clause 5.4.2.1-1 of TS 23.401 [6] are executed to update QoS in the UE and the RAN.

7-8. [Optional] The PCF sends Npcf_PolicyAuthorization_Notify message to the UAS NF/NEF when the modification of the transmission resources corresponding to the QoS update succeeded or failed. The UAS NF/NEF transfers this information to the USS by sending Nnef_AFSessionWithQoS_Notify message. See steps 6 and 7 in figure 4.15.6.6-1 of TS 23.502 [3].

5.2.6 Void

5.2.7 UUAA Revocation by USS/UTM

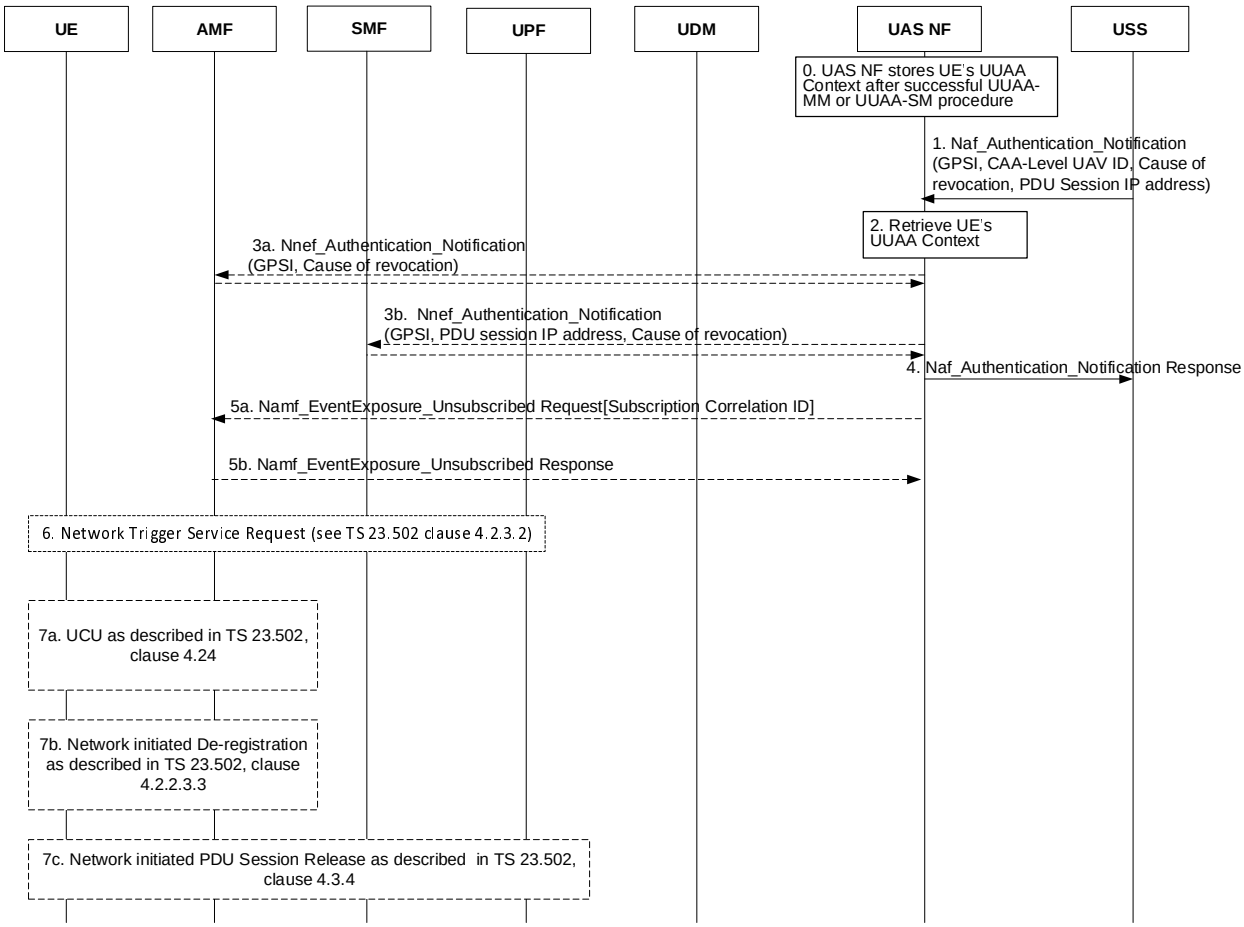

Figure 5.2.7.1-1: Procedure for UAV authorization revocation by USS

UAS NF stores the UAV UE's UUAA context after successful UUAA procedure as explained in clause 5.2.2.2 for UUAA-MM and in clause 5.2.3.2 for UUAA-SM procedure.

1. The USS sends Naf_Authentication_Notification to UAS NF for authorization revocation. The USS includes GPSI, CAA-Level UAV ID, cause of revocation, PDU Session IP address if available in the authorization revocation request.

2. UAS NF retrieves the UAV UE's stored UUAA context. From the stored UUAA context the UAS NF determines the target AMF or SMF for sending the notification.

3a or 3b. The UAS NF sends Nnef_Authentication_Notification request to notify the target NF, i.e. either the AMF or the SMF that the UAV is not authorized anymore, indicating the cause is revocation. The target NF shall remove the successful UUAA result and respond to the UAS NF.

4. The UAS NF shall remove the UAV UE's UUAA context. The UAS NF responds back to the USS indicating that authorization revocation request has been successfully initiated.

5a. If UAS NF has subscribed to AMF for the Mobility Event Exposure with Event ID = Reachability Filter before, UAS NF unsubscribes to AMF for the mobility event notification by sending Namf_EventExposure_Unsubscribe request with Subscription Correlation ID.

5b. The AMF acknowledges the un-subscription request from 5a by sending Namf_EventExposure_Unsubscribe response.

6. If UE is in CM_Idle state, the target NF (i.e. either the AMF or the SMF) initiates the Network Triggered Service Request procedures as described in clause 4.2.3.3 of TS 23.502 [3].

7a. If the target NF is AMF, the AMF initiates UCU procedure to inform the UE that UUA is revoked. The AMF shall also initiate the release of PDU Sessions related to UAS services.

7b. If the target NF is AMF, based on network policy the AMF may start network initiated de-registration process as described in clause 4.2.2.3.3 of TS 23.502 [3].

7c. If the target NF is SMF, the SMF starts network initiated PDU session release process as described in clause 4.3.4 of TS 23.502 [3] to release the associated PDU session.

5.2.8 UAV Controller Replacement

5.2.8.1 UAV controller replacement in 5GS

If USS determines that UAV controller replacement is required the USS invokes an Nnef_AFsessionWithQoS_Update service operation to the UAS NF including in the request authorization information (i.e. new pairing information). NEF authorizes the request from the USS followed by interacting with PCF triggering a Npcf_PolicyAuthorization_Update request and provides relevant parameters to the PCF. The PCF uses the information provided by the NEF to derive new PCC rules to allow C2 communication between the UAV and the new UAV controller.

The procedure for UAV-C replacement is as follows:

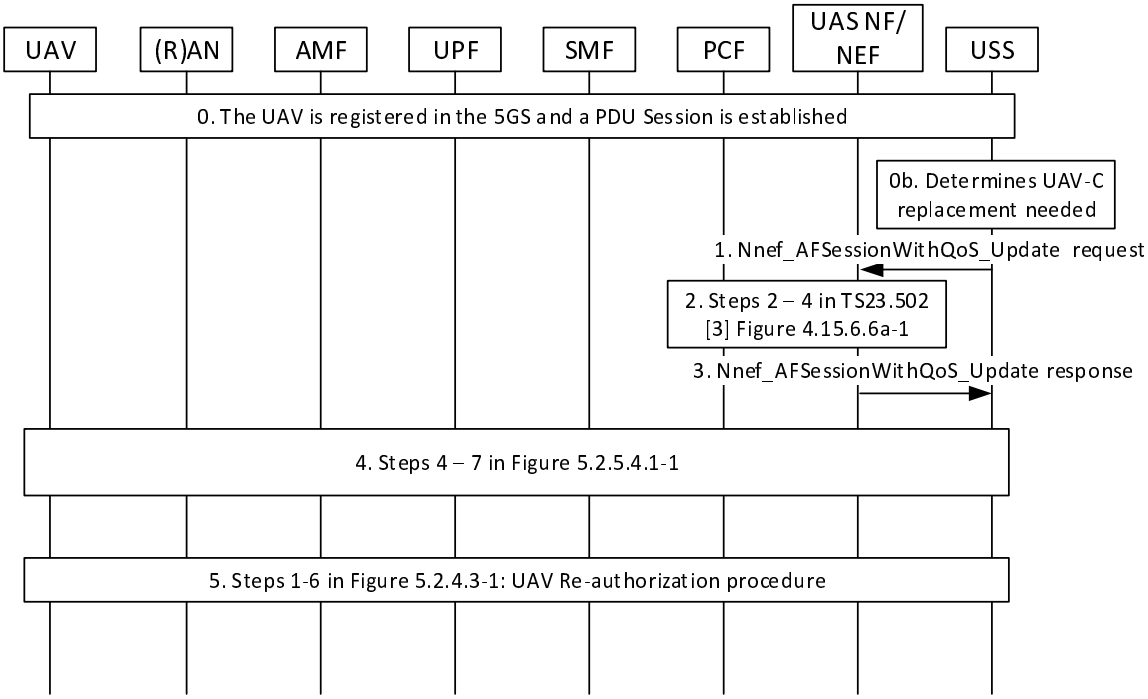

Figure 5.2.8-1: UAV-C replacement procedure

0. A UAV has already established user plane connectivity for C2 operation. The USS determines that the UAV-C controlling the UAV needs to be replaced (e.g. if the UAV is misbehaving).

1. The USS initiates the UAV-C replacement by invoking the Nnef_AFSessionWithQoS_Update request including Transaction Reference ID, UAV-UAVC Pairing info/Flow description(s), QoS reference. See step 1 in TS 23.502 [3] clause 4.15.6.6a, AF session with required QoS update procedure.

2. NEF authorizes the request from the USS followed by interacting with PCF triggering a Npcf_PolicyAuthorization_Update request and provides relevant parameters to the PCF. PCF determines whether the request is authorized and if the requested QoS is allowed. PCF informs NEF if the request is accepted by invoking Npcf_PolicyAuthorization_Update Response. See Steps 2 - 4 in TS 23.502 [3] figure 4.15.6.6.6a-1.

3. NEF sends a Nnef_AFsessionWithQoS_Update response message (Transaction Reference ID, Result) to the USS. Result indicates whether the request is granted or not. See step 5 in TS 23.502 [3] figure 4.15.6.6.6a-1.

4. Steps 4 - 7 in Figure 5.2.5.4.1-1.

5. USS invokes the UAV Re-authorization procedure in Figure 5.2.4.3-1 to deliver the new pairing information to the UE. The USS includes the 3GPP UAV ID, the IP address of the PDU session and included in the authorization message the C2 Authorization Result and the C2 Authorization Payload (containing the C2 pairing information containing the new UAV-C identifier and C2 security information) which is further forwarded to the UE.

5.2.8.2 UAV controller replacement in EPS

The procedure for UAV-C replacement in EPS is as follows:

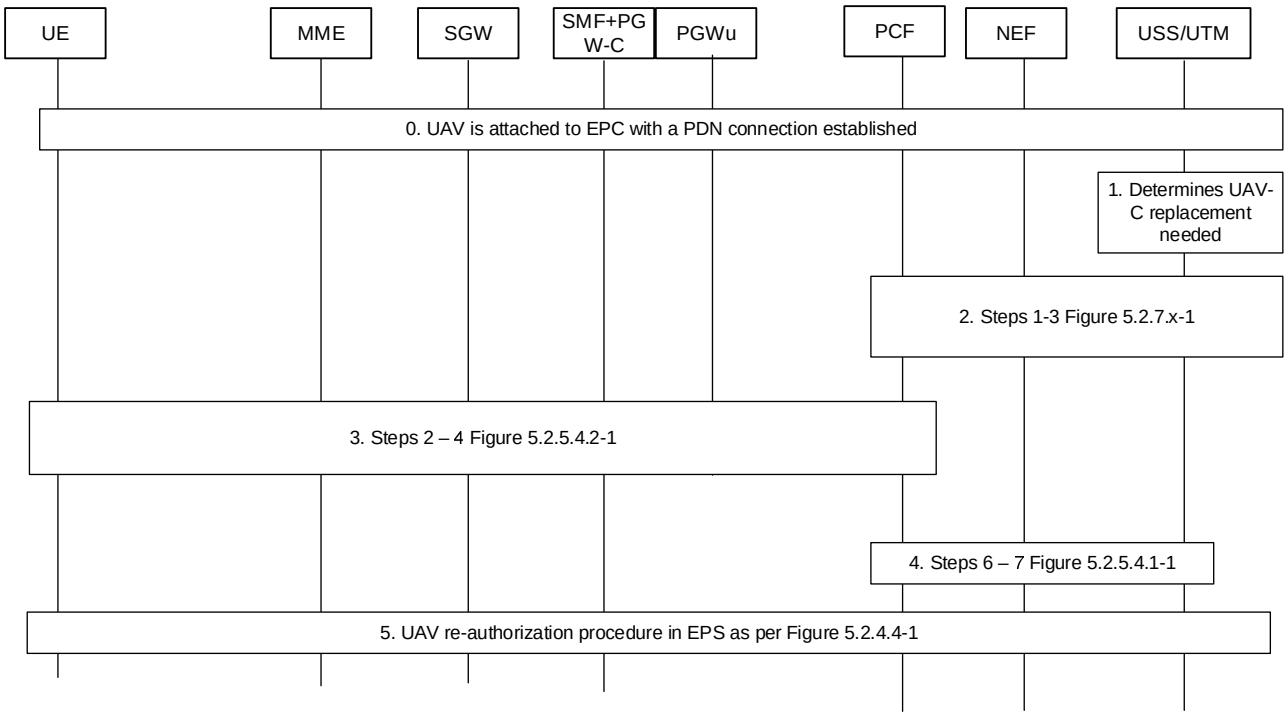

Figure 5.2.8.2-1: UAV controller replacement in EPS

0. UAV is attached to EPC with a PDN connection established

1. The USS determines that the UAV-C controlling the UAV needs to be replaced (e.g. if the UAV is misbehaving).

2. USS initiates the Nnef_AFSessionWithQoS_Update request including USS Identity/AF Identifier, Transaction Reference ID, UAV-UAVC Pairing info/Flow description(s), QoS reference. Steps 1-3 as in Figure 5.2.7.1-1 takes place.

3. The PCF determines updated policy information and configures the resources and routing information as in steps 2 - 4 in Figure 5.2.5.4.2-1.

4. The USS is informed whether the UAV-C replacement and authorization has succeeded or failed as in steps 6- 7 in Figure 5.2.5.4.1-1.

5. The USS invokes the UAV re-authorization procedure in EPS as in Figure 5.2.4.4-1. The USS includes the 3GPP UAV ID, the IP address of the PDU session and included in the authorization message, the C2 Authorization Result and the C2 Authorization Payload (e.g. containing the C2 pairing information containing the new UAV-C identifier and C2 security information) which is further forwarded to the UE.

5.2.9 Revocation of C2 Connectivity

5.2.9.1 Revocation of C2 connectivity in 5GS

When the USS decides to revoke an existing C2 connection between the UAV and UAV-C the USS invokes an Nnef_AFsessionWithQoS_Revoke request to NEF in order to revoke the AF request as described in Figure 5.2.9.1-1.

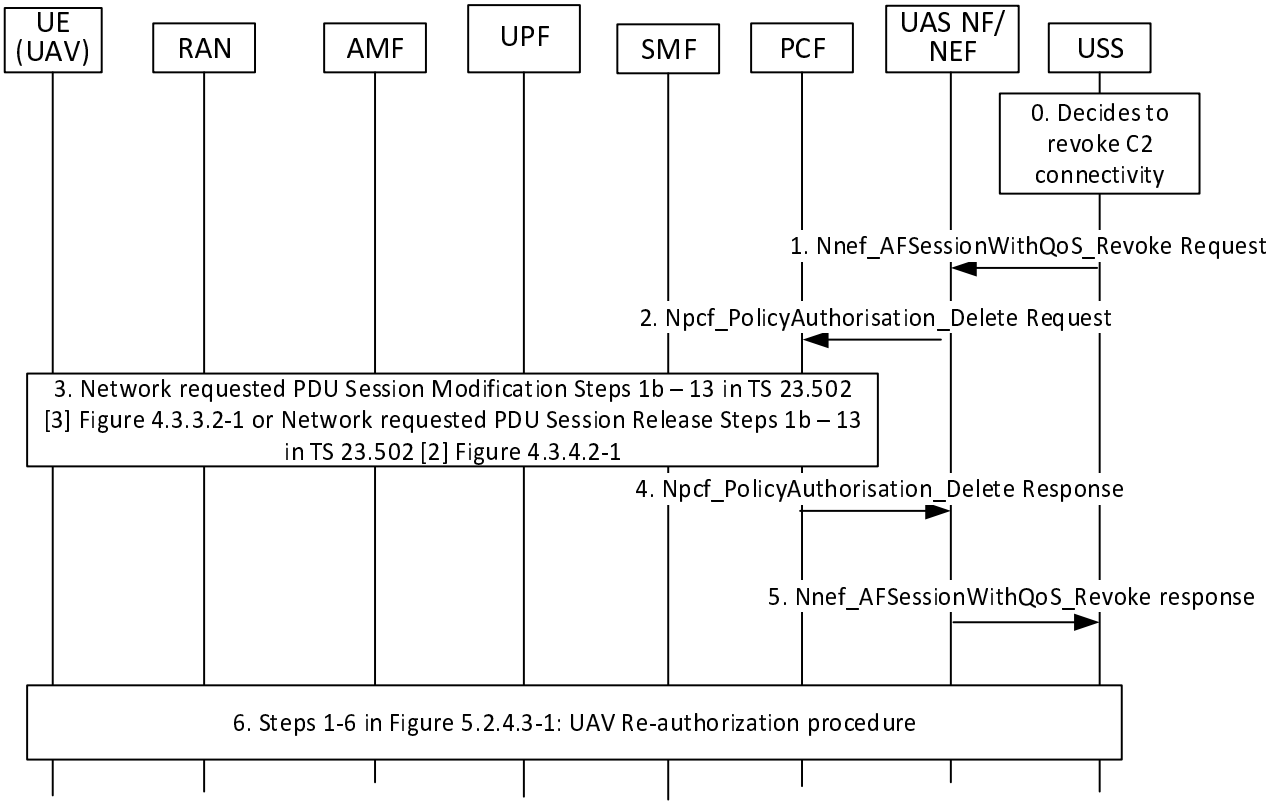

Figure 5.2.9.1-1: Revocation of C2 connectivity in 5GS

0. USS decides to revoke C2 connectivity.
1. USS identifies the AF session corresponding to the C2 connectivity and invokes an Nnef_AFSessionWithQoS_Revoke Request including USS identity/AF identifier, Transaction Reference ID.
2. UAS NF/NEF indicates to the PCF to delete the context of application level session information by invoking an Npcf_PolicyAuthorization_Delete request.
3. The PCF initiates a network requested PDU session modification procedures as in steps 1b-13 in Figure 4.3.3.2-1 of TS 23.502 [3] removing the corresponding PCC rules installed at the SMF to support the AF session or may trigger a network requested PDU session release as in Steps 1b-13 Figure 4.3.4.2-1 of TS 23.502 [3].
4. The PCF acknowledge the request by sending an Npcf_PolicyAuthorization_Delete response.

NOTE: Steps 3 and 4 can be carried out in parallel.

5. The UAS NF/NEF acknowledge the USS request by sending an Nnef_AFSessionWithQoS_Revoke response.
6. USS may invoke the UAV Re-authorization procedure in Figure 5.2.4.3-1 to deliver a C2 authorization payload indicating that C2 authorization has been revoked.

5.2.9.2 Revocation of C2 connectivity in EPS

The procedure is as follows:

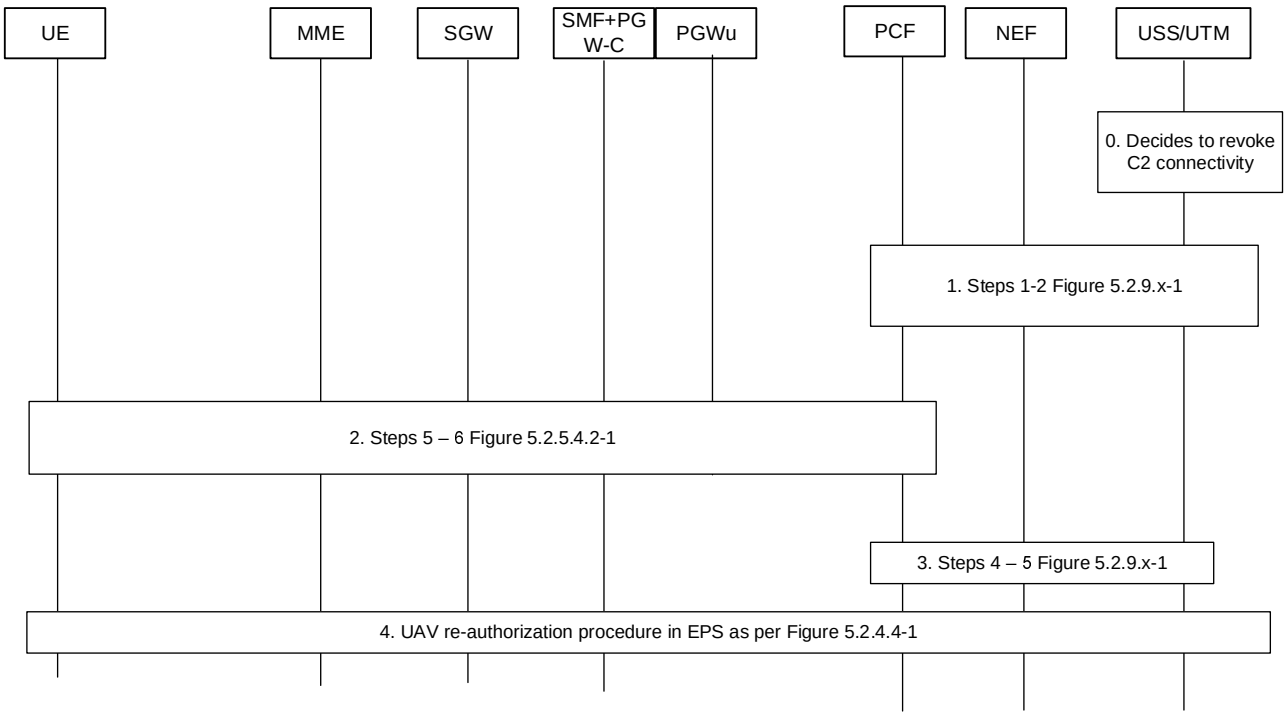

Figure 5.2.9.2-1: Revocation of C2 connectivity in EPS

0. USS decides to revoke C2 connectivity.
1. Steps 1 - 2 as described in Figure 5.2.9.1-1 are performed.
2. The PCF deletes policy information associated with the AF session and configures the resources and routing information as in steps 5 - 6 in Figure 5.2.5.4.2-1.
3. Steps 4-5 as described in Figure 5.2.9.1-1 are performed.

NOTE: Step 2 in Figure 5.2.9.2-1 and step 4 in Figure 5.2.9.1-1 can be carried out in parallel.

4. The USS may invoke the UAV re-authorization procedure in EPS as in Figure 5.2.4.4-1 to deliver a C2 authorization payload indicating that C2 connectivity is revoked.

5.3 UAV Tracking

5.3.1 UAV Tracking Model

3GPP network supports the functionality of UAV Tracking via the service exposure support towards USS. The USS invokes 3GPP network service through a UAS-NF for UAV tracking. The UAS-NF acts as an NEF/SCEF and interacts with other network functions (e.g. GMLC and AMF/MME) to support UAV tracking. The USS shall use 3GPP UAV ID (e.g. GPSI) for identifying an individual target UAV. When USS/TPAE initiates UAV tracking via USA NF, it should include an indication of reliable UE location information required in the request. For further details on the architecture reference model, see clause 4.2.

Three UAV tracking modes are supported:

- UAV location reporting mode;
- UAV presence monitoring mode; and
- List of Aerial UEs in a geographic area..

USS/TPAE could at any time choose a UAV tracking mode and provide the corresponding request to UAS NF. The USS/TPAE logic on its choice of UAV Tracking Model is out of scope of 3GPP.

The 3GPP network may also provide the UAV location to the USS during the UUAA procedures, as described in clause 5.2.2 and clause 5.2.3.

5.3.1.1 UAV Location Reporting Mode

For UAV location reporting mode, the USS/TPAE that wants to be reported on the UAV location subscribes to the UAS NF with the target 3GPP UAV ID. The USS/TPAE could indicate the required location accuracy, reliable UE location information required and whether it's for immediate reporting or deferred reporting (e.g. periodic reporting). With the request received from USS/TPAE, UAS NF identifies the related NF, i.e. GMLC and trigger existing procedures to retrieve the location report. Then UAS NF reports back the UAV's location together with the 3GPP UAV ID to the USS/TPAE.

5.3.1.2 UAV Presence Monitoring Mode

For UAV presence monitoring mode, the USS/TPAE may subscribe for the event report of UAV moving in or out of the geographic area (e.g. longitude/latitude, zip code, etc). The request includes target 3GPP UAV ID, indication of reliable UE location information required and geographic area info.

If the requested geographic area info can be mapped to 3GPP defined area, such as a list of Tracking Areas or a list of cells as currently supported by 3GPP network as the Area Of Interest, UAS NF subscribes to AMF/MME for reporting the presence of the UAV in Area Of Interest using existing AMF/MME procedures, otherwise UAS NF subscribes to GMLC for configuring the presence monitoring. Upon receiving the report from AMF/MME or GMLC, the UAS NF notifies USS/TPAE for the UAV presence in the geographic area.

The USS may provide policies or rules to UAS NF based on the received event notification. If the traffic routing policies or rules were provided to UAS NF, when the location of UAV or the UAV presence in the monitoring area matches a policy, UAS NF based on the policy indicates SMF to take the appropriate network layer actions, e.g. revoke the connectivity between UAV and UAV controller. UAS NF considers those policies as active and ongoing instructions from USS without constant or repeated triggers/requests from USS. The traffic routing policy includes 3GPP UAV ID(s) (i.e. GPSI(s)) to identify the UAV(s) and the corresponding network layer actions e.g. revoke the resources of the related C2 communications.

5.3.1.3 List of Aerial UEs in a geographic area

In this mode, the USS/TPAE requests UAS NF for a list of the UAVs in the geographic area and served by the PLMN (i.e. no 3GPP UAV ID provided by the USS/TPAE). The request includes geographic area info, indication of reliable UE location information required and indication of one-time reporting by setting "maximumNumberOfReports" to 1. If the geographic area info can be mapped to 3GPP defined area such as a list of Tracking Areas or a list of cells, UAS NF triggers existing AMF/MME procedures to get the UE list within the TAI(s) or Cell Id(s). The UAS NF may include Aerial UE indication as an event filter in the request, that is used by the AMF/MME to separate out the UEs that are actual UAVs based UEs with aerial subscriptions. If the geographic area info cannot be mapped to 3GPP defined area such as a list of Tracking Areas or a list of cells, UAS NF provides a list of Tracking Areas which is larger than the geographic area to AMF/MME to retrieve the UE list within the list of Tracking Areas. Then UAS NF identifies UAVs from the UE list and obtains the location for each identified UAV via LCS procedure toward GMLC. The UAS NF compares the UAV location with the geographic area to identify the UAVs in the geographic area and provides feedback to USS/TPAE. For the UAV list received from the AMF/MME or the UAV list identified with GMLC provided location, the UAS NF performs the filtering by checking for each 3GPP UAV ID reported whether there is match for the corresponding UAV context. The UAS NF may also verify whether the requesting USS is authorized to obtain the location info of the UAV.

In the above UAV tracking modes, UAS NF may need to map the 3GPP UAV ID to 3GPP internal IDs and vice versa. The CAA Level UAV ID may be optionally provided by the UAS NF, if available, to the USS/TPAE during tracking and location reporting of UAV.

5.3.2 Procedure for UAV location reporting

The following procedures describe the 5GC UAV's location reporting service to USS.

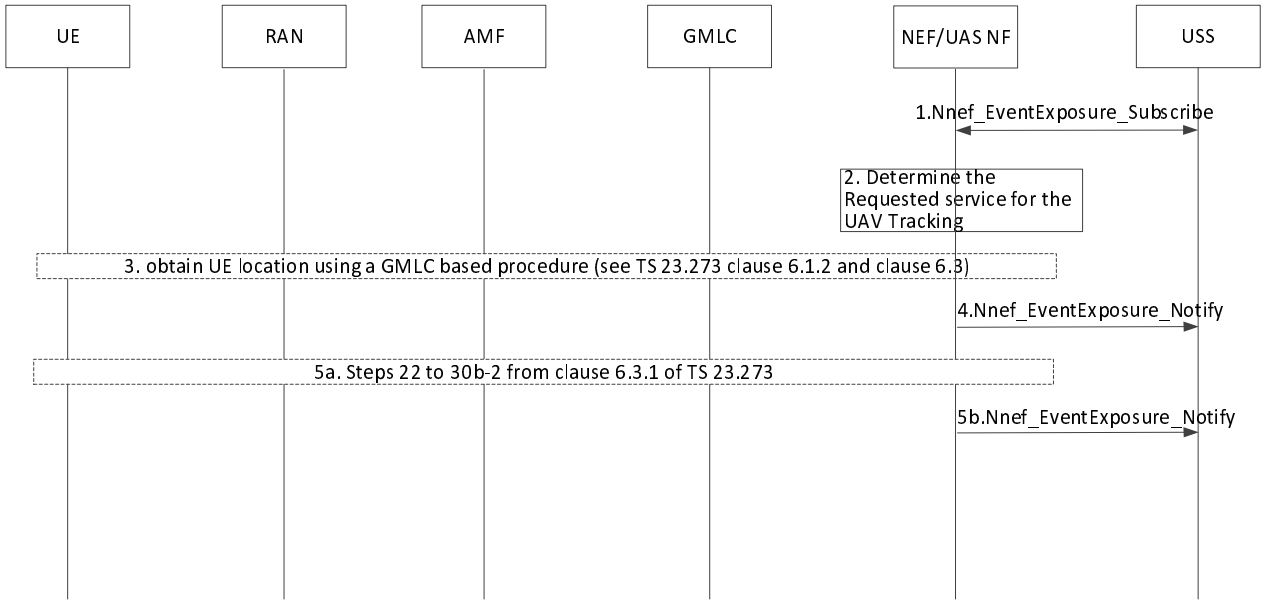

Figure 5.3.2-1: UAV Location Reporting

1. USS to UAS NF/NEF: The USS sends Nnef_EventExposure_Subscribe request to the UAS NF/NEF as described in step 1b-1 from clause 6.1.2 of TS 23.273 [8] for immediate location reporting (i.e. 5GC-MT-LR) and step 1b-1 from clause 6.3.1 of TS 23.273 [8] for periodic, triggered and UE available location reporting (i.e. deferred 5GC-MT-LR). USS should include an indication of reliable UE location information required in the request.

2. UAS NF/NEF determines the relevant NF, i.e. GMLC for location reporting based on the UAV's capability or network capability, location accuracy etc.

3. UAS NF sends request to GMLC with the GPSI (i.e. 3GPP UAV ID) provided by USS to retrieve the UE location via the current location services supported by GMLC. The UAS NF/NEF performs 5GC-MT-LR Procedure as described in clause 6.1.2 of TS 23.273 [8] or deferred 5GC-MT-LR procedure as described in clause 6.3.1 (up to step 21b-1) of TS 23.273 [8] depending on whether the request received in step 1 was for immediate location reporting or deferred location reporting respectively.

4. UAS/NEF NF to USS: UAS NF/NEF provides the UAV location to USS/TPAE in Nnef_EventExposure_Notify operation as described in step 24b-2 of Figure 6.1.2-1, if the request in step 1 was for immediate location reporting. The UAS NF/NEF includes the GPSI in the location reporting message to USS/TPAE as well as the UAV's location information (in the form of geo co-ordinates) which is understood by USS/TPAE (not assuming the knowledge of TA and Cell Id).

   If the request in step 1 was for deferred 5GC-MT-LR, the UAS NF/NEF sends Nnef_EventExposure_Notify indicating whether or not the periodic or triggered location was successfully activated in the target UE, as described in step 21b-2 of Figure 6.3.1-1.

5. For deferred 5GC-MT-LR with periodic or triggered location request steps 22 to 30b-2 of Figure 6.3.1-1 are executed and the UAS NF/NEF provides the location report to USS/TPAE in Nnef_EventExposure_Notify operation.

5.3.3 Procedure for UAV presence monitoring

The following procedures describe the 3GPP UAV presence monitoring mode operation.

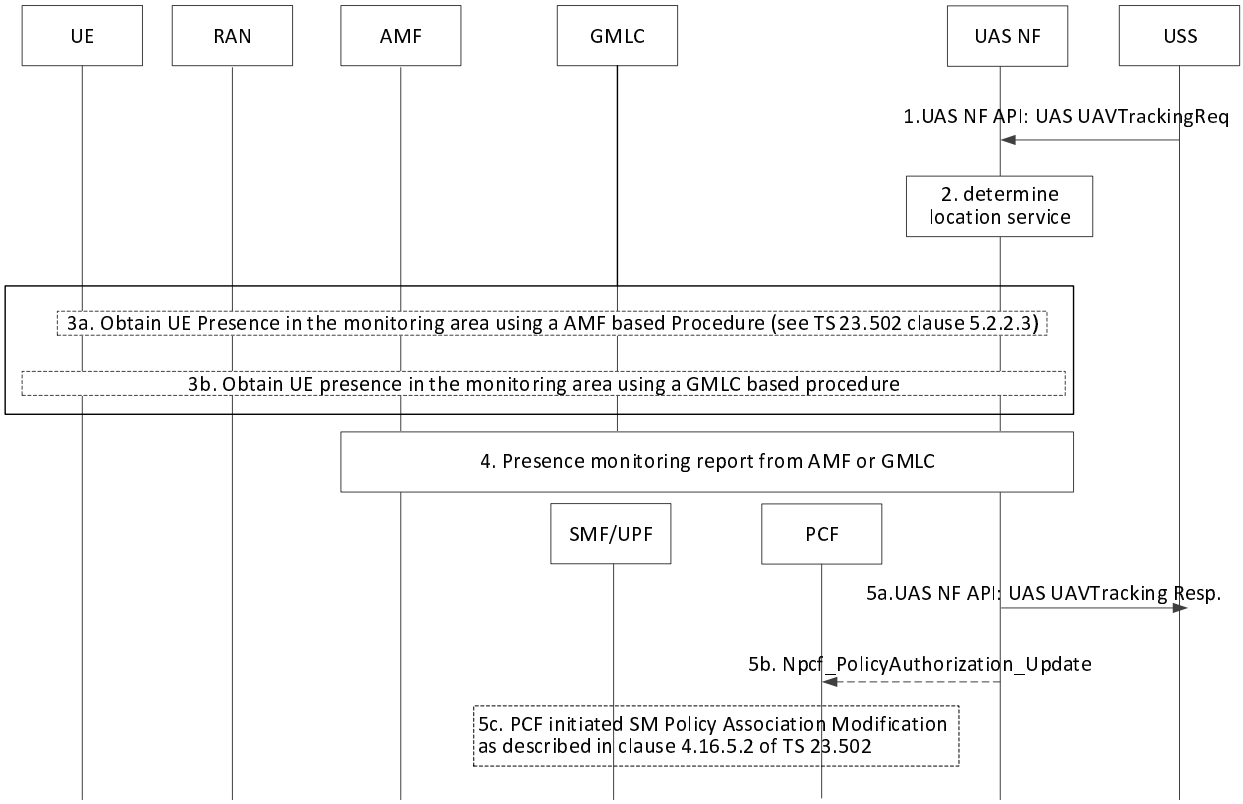

Figure 5.3.3-1: UAV Presence Monitoring

1. USS to UAS NF/NEF: The USS initiates the UAV presence monitoring request via the Nnef_EventExposure_Subscribe service operation to UAS NF/NEF to subscribe to the target UAV presence events from 3GPP network (e.g. moving in or out of the monitoring area). In addition to providing a GPSI corresponding to the target UAV for the presence monitoring, the request also includes the geographic area info (e.g. longitude/latitude, zip code, etc.), an indication of reliable UE location information required. Optionally, it includes a policy or rule indicating the 3GPP network to take the corresponding action when the Area of Interest (AOI) event report is detected. The policy or rule contains a moving in or moving out event associated with an indication of revoking the connectivity between UAV and UAV controller.

2. UAS NF/NEF maps the geographical area into an area of interest that is represented by a list of Cell IDs, gNB IDs or TAIs, and determines the relevant NF (s), i.e. AMF or GMLC for location reporting based on the UAV's capability or network capability, the geographic area info etc.

3a. If the requested geographic area info can be mapped to 3GPP defined area and the relevant NF is determined as AMF in step 2, then the UAS NF/NEF maps the GPSI provided by USS to SUPI, and provides the SUPI and the mapped 3GPP defined area to the AMF to obtain the UE presence status by reusing the Area of Interest mechanism.

3a. If the requested geographic area info cannot be mapped to 3GPP defined area and the relevant NF is determined as GMLC in step 2, then the UAS NF/NEF uses GMLC based procedure for configuring the presence monitoring. It is preferrable for UAS NF/NEF to use GMLC based procedure if presence monitoring is needed in a granularity finer than the Cell Id. The UAS NF/NEF invokes an Ngmlc_Location_ProvideLocation Request service operation towards the GMLC including the geographical area of interest for presence monitoring. The UAS NF/NEF may first use AMF based procedure for UE presence monitoring as described in step 3a before invoking GMLC service.

4. UAS NF/NEF receives the UAV presence monitoring report from AMF or GMLC.

5a. UAS NF/NEF reports the UAV presence in the geographic area to USS by including its GPSI in the report. The CAA Level UAV ID, if available with the UAS NF/NEF, may be optionally provided in the report.

5b-5c. [Optional] If policies have been provided to UAS NF/NEF in step1 from USS, when the UAV presence in the monitoring area matches a policy, UAS NF/NEF based on the policy indicates SMF (via PCF) to take the appropriate network layer actions, e.g. revoke the connectivity between UAV and UAV controller, etc. The UAS

NF/NEF uses the Npcf_PolicyAuthorization_Update service operation as described in clause 4.15.6.6.6a of TS 23.502 [3] and provides relevant parameters to the PCF. UAS NF/NEF considers those policies as active and ongoing instructions from USS without constant or repeated triggers/requests from USS. The PCF issues a Npcf_SMPolicyControl_UpdateNotify request with updated policy information received from the UAS NF/NEF about the PDU Session as described in the PCF initiated SM Policy Association Modification procedure in clause 4.16.5.2.

5.3.4 Procedure for obtaining list of Aerial UEs in a geographic area

This procedure may be used by USS/TPAE to obtain a list of the UAVs in a geographic area and served by the PLMN. The USS/TPAE provides the geographic area information to the UAS-NF. Based on the received information, the UAS NF may either trigger the AMF/MME monitoring event configuration procedure with event ID "Number of UEs present in a geographical area" or the GMLC based location reporting procedure. The AMF/MME may filter the list of UAVs before sending it to the UAS NF (e.g. may filter only based on UE having Aerial subscription), if Aerial UE indication was included as an event filter in the monitoring event configuration request from the UAS NF. The UAS NF performs the filtering on the received list from AMF or MME before responding back to the USS/TPAE. The UAS-NF includes the 3GPP UAV ID and may include the CAA Level UAV ID, if available, for each of the UAVs in the tracking and location response to the USS/TPAE.

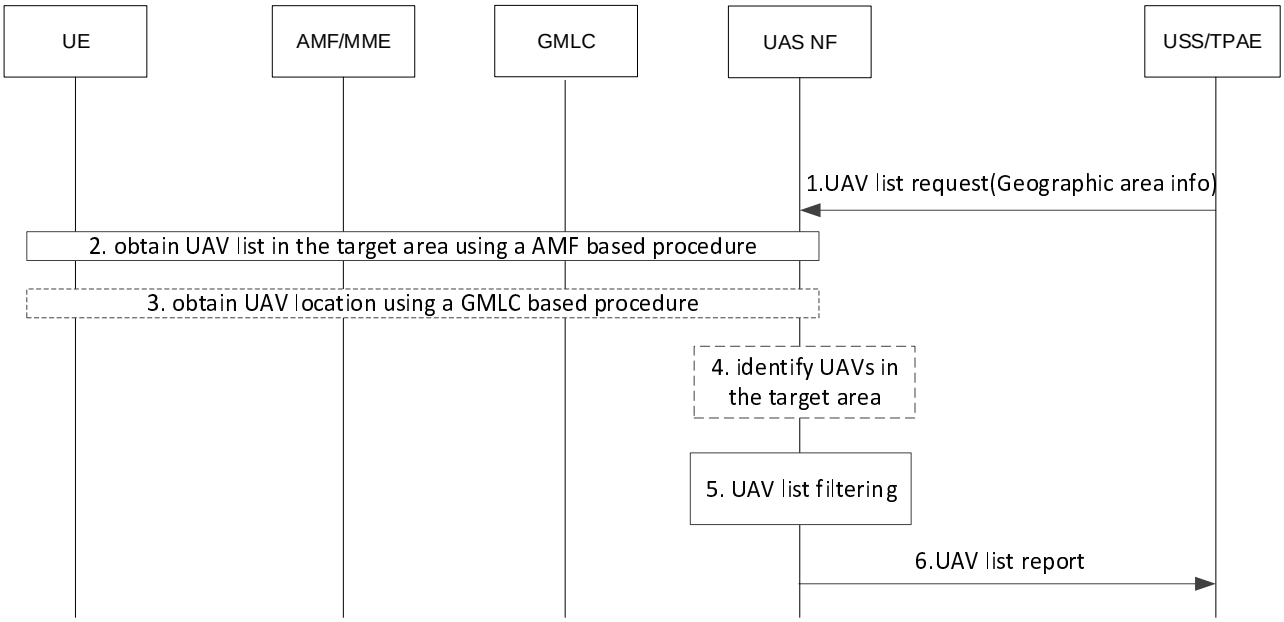

Figure 5.3.4-1: List of Aerial UEs in a geographic area

1. USS to UAS NF: The USS/TPAE sends the UAV list request to UAS NF to request UAV identity (e.g. 3GPP UAV ID, CAA Level UAV ID). The USS/TPAE includes geographic area info, an indication of reliable UE location information required and indication for immediate reporting in the request message to the UAV-NF.

2. UAS NF to AMF/MME: UAS NF decides the AMF(s) based on the geographic area info and obtains the UE list in the target area from AMF by reusing the event "Number of UEs present in a geographical area" with any UE in the event filter. The UAS NF may also include "Aerial UE" indication and/or "PDU session established for DNN(s) subject to aerial service" as event filters. If the target area cannot be mapped to 3GPP network areas, UAS NF provides a TA List which is larger than the target area to the AMF(s)/MME(s) for the list of UEs to be queried. The AMF(s)/MME(s) identifies UEs corresponding to the geographic area info and may also filter out the list of UAVs based on checking for UEs with aerial subscriptions, if "Aerial UE" indication was included as an event filter in the request from UAS NF/NEF. In addition, the AMF(s) may also further identify UAVs that have successfully established PDU session for DNN(s) subject to aerial services, if it was included as an event filter in the request from UAS NF/NEF.

3. [Optional] UAS NF to GMLC: From the list of UEs generated in step 2, for UAVs that are in target areas that do not map to 3GPP network areas, the UAS-NF then queries the UAV(s) location from GMLC.

4. [Conditional] If step 3 above was executed, from the list of locations returned by the GMLC, the UAS NF compares the UAV's locations to the target area (provided in step 1 above) to identify the UAV to be included in the report for USS.

5. For either the UAV list received from the AMF(s)/MME(s), or the UAV list identified in step 4, the UAS NF performs the filtering by checking for each reported 3GPP UAV ID whether there is match for the corresponding UUAA context.

6. UAS NF to USS: UAS NF responds to the USS/TPAE with the list of filtered UAVs (step 5). The CAA Level UAV ID, if available, may be provided by the UAS NF in the response message to USS/TPAE. If the USS performed the UUAA of the UAV, or the UAS NF is configured to know the USS is authorized to receive such information, then the 3GPP UAV ID is also included.

Annex A (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2021-02	SA2#143-e	S2-2101029	-	-	-	TS skeleton (approved in S2-2101029)	0.0.0
2021-06	SA#92E	SP-210366	-	-	-	MCC editorial update for presentation to TSG SA#92E for information	1.0.0
2021-09	SA#92E	SP-210939	-	-	-	MCC editorial update for presentation to TSG SA#93E for approval	2.0.0
2021-09	SA#92E	-	-	-	-	MCC editorial update for publication after TSG SA#93E approval	17.0.0
2021-12	SA#94E	SP-211297	0002	2	F	Clarification and EN resolution for SMF Services	17.1.0
2021-12	SA#94E	SP-211297	0003	1	F	Clarifications for UUAA-SM procedure	17.1.0
2021-12	SA#94E	SP-211297	0004	1	F	UUAA during default PDN connection at Attach	17.1.0
2021-12	SA#94E	SP-211297	0005	-	F	USS Initiated procedures update	17.1.0
2021-12	SA#94E	SP-211297	0006	1	F	C2 Authorization for EPS	17.1.0
2021-12	SA#94E	SP-211297	0007	-	F	23.256 clean-up	17.1.0
2021-12	SA#94E	SP-211407	0008	2	F	Clean up for List of Aerial UEs in a geographic area	17.1.0
2021-12	SA#94E	SP-211297	0009	1	F	UUAA-MM Procedure Updates	17.1.0
2021-12	SA#94E	SP-211297	0010	3	F	Clarification and Correction on AF and NEF authentication service	17.1.0
2021-12	SA#94E	SP-211297	0011	2	F	Clarify the implicit subscription during the UUAA procedure	17.1.0
2021-12	SA#94E	SP-211297	0012	1	F	Clarification on UUAA-MM failure	17.1.0
2021-12	SA#94E	SP-211297	0013	1	F	Clarification on AMF and SMF addressing UAS NF/NEF	17.1.0
2021-12	SA#94E	SP-211297	0014	-	F	Correction on new CAA-level UAV ID allocation	17.1.0
2021-12	SA#94E	SP-211297	0015	1	F	Correction on UAV tracking mode	17.1.0
2021-12	SA#94E	SP-211297	0016	1	F	Association of CAA level UAV ID to 3GPP UAV ID in USS	17.1.0
2021-12	SA#94E	SP-211297	0020	1	F	Procedure for UAV replacement in EPS	17.1.0
2021-12	SA#94E	SP-211297	0022	-	F	Miscellaneous corrections	17.1.0
2021-12	SA#94E	SP-211298	0024	1	F	Correction on UUAA re-authentication and re-authorization procedure	17.1.0
2021-12	SA#94E	SP-211298	0026	1	F	Correction and simplification on UAV-C replacement procedure	17.1.0
2021-12	SA#94E	SP-211298	0028	1	F	UAS architecture figure update for IWK	17.1.0
2021-12	SA#94E	SP-211298	0030	1	F	TS 23.256: various clarifications and corrections	17.1.0
2021-12	SA#94E	SP-211298	0031	3	F	TS 23.256: Rapporteur Editorial CR	17.1.0
2021-12	SA#94E	SP-211298	0032	1	F	Correction of UUAA when aerial subscription is missing	17.1.0
2021-12	SA#94E	SP-211298	0035	1	F	Clean up for UUAA-MM procedure	17.1.0
2021-12	SA#94E	SP-211298	0036	1	F	Replace of the term pairing authorization	17.1.0
2021-12	SA#94E	SP-211298	0038	1	F	Clarifications on UUAA context during revocation procedure	17.1.0
2021-12	SA#94E	SP-211298	0039	1	F	Clarifications and corrections on UAV Re-authentication	17.1.0
2021-12	SA#94E	SP-211298	0040	1	F	Correction on UAS NF discovery and UAS NF functionality	17.1.0
2021-12	SA#94E	SP-211298	0044	-	F	Corrections on usage of Nnef_AFsessionWithQoS service for UAS	17.1.0
2022-03	SA#95E	SP-220059	0048	-	F	Clarification on cause of revocation	17.2.0
2022-03	SA#95E	SP-220059	0049	1	F	UUAA context management	17.2.0
2022-03	SA#95E	SP-220059	0051	1	F	Clarification on PDU Session Status Event	17.2.0
2022-03	SA#95E	SP-220059	0052	1	F	Clarification on UAV Re-authorization procedure	17.2.0
2022-03	SA#95E	SP-220059	0054	1	F	Revocation of C2 authorisation	17.2.0
2022-03	SA#95E	SP-220059	0055	1	F	Correction on handling the authorized CAA-Level UAV ID provided by a USS	17.2.0
2022-03	SA#95E	SP-220059	0056	1	F	Clarification on re-authorization	17.2.0
2022-03	SA#95E	SP-220059	0057	1	F	Corrections to Nnef_Authentication_AuthenticateAuthorize service operation	17.2.0
2022-06	SA#96	SP-220403	0059	1	F	Correcting errors for UAV-C address	17.3.0
2022-06	SA#96	SP-220403	0062		F	Corrections to Naf(Nnef)_Authentication_AuthenticateAuthorize service operation	17.3.0
2022-06	SA#96	SP-220403	0063	1	F	Clarification and Correction on C2 payload	17.3.0
2022-06	SA#96	SP-220403	0064	1	F	Corrections to service operation names	17.3.0
2022-09	SA#97E	SP-220782	0065	1	F	Clarifications on subscription control for UUAA-SM and C2 authorization	17.4.0
2022-09	SA#97E	SP-220782	0067		F	Correction on reference on UAV re-authentication procedure in 5GS	17.4.0
2022-12	SA#98E	SP-221075	0068	2	F	Corrections to functionality and procedure at UAS NF for C2 authorization	17.5.0
2022-12	SA#98E	SP-221075	0069	1	F	Indication of Network Assisted Positioning method for UAV positioning	17.5.0
2022-12	SA#98E	SP-221333	0072	1	F	Aerial Service Availability Update using UCU	17.5.0
2023-03	SA#99	SP-230041	0073	1	F	Addressing Editor Notes	17.6.0
2023-12	SA#102	SP-231244	0112	-	F	Cleanup of UUAA-MM and UUAA-SM relation	17.7.0

History

Document history		
V17.2.0	May 2022	Publication
V17.3.0	July 2022	Publication
V17.4.0	September 2022	Publication
V17.5.0	January 2023	Publication
V17.6.0	April 2023	Publication
V17.7.0	January 2024	Publication