UAV authentication/ authorization mechanism by the USS/UTM during PDU session establishment uses a “Generic DN authentication/ authorization mechanism”; this paper proposes a sub work plan on how to address this in terms of 3GPP documentation. The proposals only focus on UAV Authentication/authorization done at PDU session (PDN connection for EPS) establishment.

**Proposal 1: endorse**

1. The UAV authentication/ authorization mechanism by the USS/UTM uses a “Generic DN authentication/ authorization mechanism” which can thus be used by other use cases.
2. This “Generic DN authentication/ authorization mechanism” should work like 23.501 § 5.6.6 “Secondary authentication/authorization by a DN-AAA server during the establishment of a PDU Session” BUT without using EAP and AAA mechanisms. Instead it relies on SMF using API towards the external authentication/ authorization entity.
3. For a single (DNN, S-NSSAI) the DN-AAA and the SBI based Secondary authentication/authorization mechanisms are exclusive for a specific DNN/S-NSSAI: but an UE can have a PDU Session to a (DNN, S-NSSAI) that requires one e.g. the AAA mechanism while another PDU to another to another (DNN, S-NSSAI) requires the other e.g. the generic (SBA) mechanism. Must be clarified UE behaviour wrt one or the other authentication mechanism, and what information the UE needs to be configured with and how the UE knows which mechanism will be used for a DNN/S-NSSAI
4. This “Generic DN authentication/ authorization mechanism” encompasses SMF, (AMF), UE but NOT the UAS NF (i.e. to interface with USS/UTM); the API interface towards USS/UTM (via an intermediate entity) is described as using NEF and SMF API (TR conclusions reads:  « The UAS-NF makes use of « existing» NEF/SCEF exposure services for UAV authentication/authorization »).

**Proposal 2: endorse**

23.501 and 23.502 document the Generic DN authentication/ authorization mechanism including

1. exchange between UE and SMF of corresponding authentication related information (assumed to be generic container in NAS SM)
2. SMF usage of NEF API(s) to request Generic DN authentication/ authorization or to receive Generic DN authorization update or Generic DN re-authentication requests
3. SMF local policy and possibly UDM subscription data to request the feature to apply on a PDU Session
4. AMF is transparent to Generic DN authentication/ authorization mechanisms
5. Ensure container is flexible to be processed by SMF for future applications: for UAS it is transparent, for other cases it may not. Issue of CAA-level UAV ID being part of container or separate, we should leave flexibility to stage 3 to code things the best way they think. SA2 states what information is carried and which network functions use. Container may have different payloads for UUAA, C2 a/a, Flight authorization. The “payloads” considered so far are CAA-level UAV ID, UUAA payload, C2 authorization payload, flight authorization payload. SMF does not need to understand C2 authorization and flight authorization payload. Note that SMF needs to be aware of result of such procedures, how needs to be defined. We need to specify what UE needs to include.

**Proposal 3: endorse each following bullet**

1. The new 23.256 is to contain the overall authentication/ authorization with
* Generic DN authentication/ authorization shown as a box referring to 23.502 message flow; the new 23.256 focuses on:
	+ UAS NF interfacing with USS/UTM, discovering it, using CAA-Level-ID and also on giving the global picture such as invoking PCF
	+ IF AMF has carried out UUAA it tells SMF and SMF does not need to carry out UUAA. This overrules SMF local policy and possibly UDM subscription data for authentication but not for SM level authorization (e.g. C2 authorization).
	+ The data that the USS/UTM may need to send via SMF to the UAV such as RITI (Remote Identification and Tracking Identification)
1. The high-level description of Generic DN authentication/ authorization is in 23.501 § 5.6.6 that is being reworded and made generic to support the two cases of DN-AAA and Generic DN authentication/ authorization.
2. The 2 features ( “Generic DN authentication/ authorization mechanism” and 23.501 § 5.6.6 “Secondary authentication/authorization by a DN-AAA server”) are controlled in a similar way: they are triggered either by local SMF policies (associated with DNN, S-NSSAI) or by subscription data (Session Management Subscription data defined in 23.502 Table 5.2.3.3.1-1: UE Subscription data types).

The control is on a per (DNN, S-NSSAI) basis.

About SM data received from UDM, it is needed to add extra information that tells that it is not a DN-AAA authentication but a Generic DN authentication/ authorization mechanism, possibly providing new parameters for the URI to contact (when the authentication/ authorization is external) or the xxx information to determine the dedicated NF (e.g. UAS NF in UAV case)

(below is a copy the existing data defined in 23.502 Table 5.2.3.3.1-1: UE Subscription data types that needs to be updated e;g; as indicated in red)

| Secondary authentication indication | Indicates that whether the Secondary authentication/authorization (as defined in TS 23.501 [2] clause 5.6) is required for PDU Session Establishment as specified in clause 4.3.2.3. |
| --- | --- |
| DN-AAA server UE IP address allocation indication could be extended for generic SBA case | Indicates that whether the SMF is required to request the UE IP address from the DN-AAA server (as defined in TS 23.501 [2] clause 5.6) for PDU Session Establishment as specified in clause 4.3.2.3. |
| DN-AAA server addressing information. could be extended or new parameter | If at least one of secondary DN-AAA authentication, DN-AAA authorization or DN-AAA UE IP address allocation is required by subscription data, the subscription data may also contain DN-AAA server addressing information. |

1. 23.502 contains flows for the Generic DN authentication/ authorization
	1. exchange between UE and SMF of corresponding authentication related information (assumed to be generic container in NAS SM) (update of § 4.3.2.3)
	2. SMF usage of API(s) to request Generic DN authentication/ authorization or to receive Generic DN authorization update or Generic DN re-authentication requests (update of § 4.3.2.3)
2. 23.401 contains a general clause on supporting UAV including UUAA that further contains the following:
	1. usage of combo SMF+PGW-c invoking N7 and involving the UAV NF as defined in new TS 23.256, feature transparent to MME and SGW
	2. A reference to 23.256 for the full UAV feature and to 23.502 message flows for “Generic DN authentication/ authorization mechanism”
	3. Defining the new PGW data (referring to 23.502 Table 5.2.3.3.1-1) associated with this feature? For the support of UAV, the combo supports also data in 23.502 Table 5.2.3.3.1-1 (text to be added in 23.401 XXXX )

The text above goes beyond the “Generic DN authentication/ authorization mechanism”

**The following is not for endorsement, just for discussion**

UUAA (Re)Authentication does not involve PCF (PCF may be notified of the result, FFS). PCF may be involved to handle some authorization data.

SMF invokes NEF-Authentication request API (can subscribe to a NEF-notify about re-authentication and about getting the authentication result)

 The actual authentication mechanism is to be defined by USS/UTM, and may depend on different regulations. Thus the generic mechanism may need to support the exchange of multiple message back and forth bewteen UE and USS/UTM

NEF may need to send signaling to the UE via SMF (for authentication but also for authorization) : invoke an SMF service SMF-data-Transfer? (open point)

When the UE (UAV) answers , SMF needs to send the answer (for authentication but also for authorization)  to NEF : invoke a NEF-data-Transfer service ? (open point)

Re-authentication/Re-athorization is possible in both directions:

IF NEF needs to trigger a re-authentication/re-athoirization: invoke a SMF service OR a NEF-NOTIFY ?

If SMF receives a max duration for the authentication, SMF can invoke a re-authentication

(dark red is part of generic procedure , black is not and defined in 23.256)

1 SMF sends NEF-Auth request to NEF

2 NEF answers (open point)

3 a Set of SMF-data-Transfer and NEF-data-Transfer

4 NEF issues a NOTIFY (authentication answer) or NEF answers to 1 (open point)

5 UAS NF can invoke PCF-author services for authorization data that need to go via PCF

6 at any time a set of SMF-data-Transfer and NEF-data-transfer can happen