CP merger plan proposal

# Merger logistics

Staged merger proposal (updates 1, 2, 3, 4 below all impact the figure).

1. Authentication message details (step 7)
	* **S3-220182, S3-220288 -> S3-220372m**
	* **S3-220372m , S3-220288m2 -> S3-220288m3**
2. Prose authentication service operations (step 5, 6, 10)
	* **S3-220131, S3-220182, S3-220211, S3-220367 -> S3-220288m1**
3. PRUK storage/prose key retrieval (new steps after steps 8 and 10, PRUK ID in step 2,3)
	* **S3-220288 -> S3-220371m,**
	* **S3-220371m , S3-220288m3 -> S3-220288m4**
4. KAUSF naming/handling (step 7), AUSF instance (step 7), SN param (step 5):
	* **S3-220103, S3-220100, S3-220104, S3-220367, S3-220288m1 ->** **S3-220288m2**

# Authentication message details

Editor's note: Further details on authentication message handling in UE, Relay UE's AMF and AUSF are FFS.

**Papers**:

* S3-220131 (OPPO): new authentication method (neither 5G AKA nor EAP-AKA')
* S3-220182 (Huawei): based on 5G AKA and EAP-AKA'
* S3-220288 (Samsung, Interdigital, LG Electronics): based on EAP-AKA'
* S3-220372 (Ericsson): based on EAP-AKA'

**Proposal**:

* Prose authentication method based on EAP-AKA' (key hierarchy to be aligned)
* Update focused on authentication messages details i.e., expand Figure 6.3.3.3.2-1 step 7 in 33.503 v0.2.0 (S3-220372 step 7, S3-220182 step 9-14, S3-220288 step 7)

# Prose authentication service operations

Editor's note: A new service operations should be used for Prose authentication to distinguish it from primary authentication defined in 33.501, to separate the different function and service logic. This is FFS.

**Papers**:

* S3-220131 (OPPO): Nausf\_UEAuthentication\_Authenticate; Nudm\_UEAuthentication Get
* S3-220182 (Huawei): Nausf\_UEAuthentication\_**ProSe**Authenticate; Nudm\_UEAuthentication\_Get**ProSeAv**
* S3-220211(CATT): Nausf\_**ProSe**\_UEAuthentication\_Authenticate; Nudm\_**ProSe**\_UEAuthentication\_Get
* S3-220288 (Samsung, Interdigital, LG Electronics): Nausf\_UEAuthentication\_Authenticate; Nudm\_UEAuthentication Get
* S3-220367 (Ericsson): Nausf\_UEAuthentication\_**Prose**Authenticate; Nudm\_UEAuthentication\_Get**ProseAv**

**Proposal**:

* New service operations: Nausf\_UEAuthentication\_**ProSe**Authenticate; Nudm\_UEAuthentication\_**ProSe**Get
* Update focused on service operations i.e. Figure 6.3.3.3.2-1 step 5,10 and 6 in 33.503 v0.2.0
* Names updated directly in S3-220288

# PRUK storage/usage

Editor's note: Further details on the needs and usage of 5GPRUK ID are FFS.

**Papers**:

* S3-220183 (Huawei): no storage
* S3-220288 (Samsung, Interdigital, LG Electronics): storage in PAnF (PAnF key storage/retrieval service similar to AAnF)
* S3-220211(CATT): storage in UDM
* S3-220371 (Ericsson): storage in PAnF (PAnF invokes AUSF authentication service)
* S3-220375 (Ericsson): no storage

**Proposal**:

* Storage in PAnF providing a service similar to AAnF for Prose key.
* PAnF service operations: Npanf\_ProseKey\_Register (called by AUSF), Npanf\_ProseKey\_Get (called by AMF) for prose key derivation (key hierarchy to be aligned)
* Update focused on adding (based on common principles from S3-220371, S3-220288)
	+ call to PAnF service operation by AUSF for storage after PRUK generation
	+ call by AMF for prose key retrieval triggered by authentication response from AUSF or request from relay including PRUK ID

# KAUSF handling/name, AUSF instance, SN params

Editor's note: There are essentially two different KAUSF keys. Different key names should be used to avoid confusion and misleading. This is FFS.

**Papers**:

* S3-220288 (Samsung, Interdigital, LG Electronics): same KAUSF name (not latest KAUSF), AUSF instance not stored in UDM, SN params sent to AUSF
* S3-220103, S3-220100, S3-220104 (ZTE): resp. same name (not latest KAUSF), AUSF instance not stored in UDM, SN params sent to AUSF
* S3-220367 (Ericsson): K'AUSF

**Proposal**:

* With introduction of a new AUSF prose specific authentication service operation (see 2 above), it would be natural to use a different KAUSF name (e.g., K'AUSF, KAUSF\_P) for clean distinction.