**Way forward and merger proposal for ProSe CP-based solution**

**Part 1: Way forward for ProSe CP-based solution**

The following editor's notes exist in CP-based solution:

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

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

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.

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

Proposes using the following contributions for discussing CP-based solution:

|  |  |  |
| --- | --- | --- |
| [**S3-220182**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_106e/Docs/S3-220182.zip) | Resolving the ENs on authentication procedure in control plane security procedure | Huawei, HiSilicon |
| [**S3-220211**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_106e/Docs/S3-220211.zip) | pCR to TS33.503 Clause 6.3 Update security procedure over Control Plane | CATT |
| [**S3-220288**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_106e/Docs/S3-220288.zip) | Resolving EN in ProSe CP based solution | Samsung, Interdigital, LG Electronics |
| [**S3-220367**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_106e/Docs/S3-220367.zip) | SBA service operations for Prose CP based solution for L3 U2N security | Ericsson |
| [**S3-220371**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_106e/Docs/S3-220371.zip) | Prose Anchor Function to handle PRUK and PRUK ID | Ericsson |
| [**S3-220372**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_106e/Docs/S3-220372.zip) | Authentication flow over PC5 for Prose CP based solution for L3 U2N security | Ericsson |
| [**S3-220131**](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_106e/Docs/S3-220131.zip) | Address the EN on the UE-to-Network Relay security procedure over control plane | OPPO |

**Question group 1 (Related to 5GPRUK and 5GPRUK ID):**

Question1.1 Do ProSe systems need to store 5GPRUK and 5GPRUK ID?

* Yes: Samsung, Interdigital, LG, CATT, Ericsson
* No: Huawei, Ericsson

Conclusion:

Question1.2 If the answer to question1.1 is yes, where are the 5GPRUK and 5GPRUK ID stored?

* Samsung, Interdigital, LG：In AUSF or in new defined Prose Anchor Function (PAnF)
* Ericsson：In Prose Anchor Function (PAnF)
* CATT：In UDM

Conclusion:

Question1.3: If PAnF is used, how is it deployed?

* Accessed by AUSF: Samsung, Interdigital, LG
* Accessed by AMF: Ericsson

Conclusion:

**Question group 2 (Method for authenticating Remote UE):**

Question 2.1: Which methods should be used for the authentication of Remote UE?

* EAP-AKA': Samsung, Interdigital, LG, CATT, Ericsson
* 5G AKA: Huawei, CATT
* Others: OPPO

Conclusion:

**Question group 3 (Authorization for Remote UE and Relay UE):**

Question 2.1: The Relay UE is authorized by the AMF of the Relay UE. Where is the authorization information of the Relay UE stored?

Conclusion:

Question 2.2: Which entity authorizes the Remote UE? Where is the authorization information of the Remote UE stored?

Conclusion:

**Question group 4 (New service operations):**

Question 4.1: Use existing service operations or define new service operations?

Defining new service operations: Huawei, CATT, Ericsson

Conclusion:

**Question group 5 (generation of Kausf):**

Question 5.1: How to generate a Kausf that derives 5GPRUK?

Use S3-220367 as baseline?

Conclusion:

Question 5.2: How to name the Kausf that derives 5GPRUK?

Use S3-220367 as baseline?

Conclusion:

**Part 2: Merger proposal from Interdigital**

13 papers updating TS 33.503 clause 6.3.3.3

Updates grouping:

* **Group#1**: EN#1: EAP authentication details
* **Group#2**: EN#2: PRUK/PRUK ID storage/usage
* **Group#3**: EN#3: AUSF authentication service
* **Group#4**: Others: KAUSF, AUSF instance, SN params

* **ZTE**: S3-220100, S3-220103, S3-220104 (group#4)
* **OPPO**: S3-220131 (group#1)
* **Huawei**: S3-220182 (group#1), S3-220183 (group#2)
* **CATT**: S3-220211 (group#2, group#3)
* **Samsung, Interdigital, LG Electronic**: S3-220288 (groups#1-4)
* **Ericsson**: S3-220367 (group#1, group#3), S3-220371 (group#2), S3-220372 (group#1), S3-220375 (group#2)

**Merger plan proposal:**

1. S3-220288 overall merge baseline
2. Group#4:

**Merger** (trivial): S3-220100, S3-220103, S3-220104, S3-220288 -> S3-220288

1. Group#1:
   1. EAP-AKA' method: S3-220288, S3-220182, S3-220372
   2. Other method: S3-220131

**Merger candidates**: S3-220288, S3-220182, S3-220372 -> S3-220288 (EAP-AKA')

1. Group#2:
   1. PRUK/PRUK ID storage in new PAnF: S3-220288, S3-220371
   2. No PRUK/PRUD ID storage: S3-220183, S3-220375
   3. PRUK/PRUK ID storage in UDM: S3-220211

**Merger candidates**: S3-220288, S3-220371 -> S3-220288 (new PAnF)

1. Group#3:
   1. Existing AUSF Authentication service: S3-220288
   2. New AUSF Prose Authentication service: S3-220367, S3-220211

**Merger candidates**: S3-220288, S3-220371, S3-220211 -> S3-220288 (new AUSF service)