**3GPP SA3 teleconference for MBS security (2021.07.22)**

**Meeting topics:**

Discuss KIs and the potential baselines for these KIs

**Content:**

**Part one: MBS traffic protection**

* **Potential security requirements:**
* The 5GS shall support the confidentiality protection, integrity protection, and anti-replay protection of MBS traffic.
* The distribution of the keys for protection of MBS traffic between the key generator and the UE shall be confidentiality, integrity and anti-replay protected.
* The 5GS shall be able to update the keys used to protect the MBS traffic.
* Service layer or transport layer
  + Analysis of the pros and cons for each solution
    - Service layer: sol#2, 3, 8, 12--> (1) Key distribution via control plane (2) Key distribution via user plane
      * Huawei
        1. MBSF/MBSTF needs to be enhanced to support the ciphering and integrity protection. It’s the centralized function for security protection.
        2. The impact is quiet low. When UE move from source RAN to the target RAN, only legacy unicast security is involved.
        3. The security protection in service layer and protection in air interface for the PDU session may be independent. This "double ciphering" is unnecessary from a security point of view.
      * …
    - Transport layer: sol#1, 10, 13--> (1)key generated in RAN (2) KMBS-RAN  = KDF {KMBS, TMGI, RANDMBS, CountMBS, PCI, ARFCN-DL} (3) KMBS-RAN  = KDF {group token, TMGI, alg-ID, rekeying token}
      * Huawei:
        1. The MRB bearer needs to support ciphering and integrity protection.
        2. When the UE moves from a NG-RAN node that supports 5MBS to a RAN node that does not support 5MBS, the network and UE shall support switch from 5GC Shared MBS traffic delivery method to 5GC Individual MBS traffic delivery method.
        3. AS security is assumed with per group and per RAN security context and RAN determines keys. In this case, when UE moves between gNBs, how to handle security context update, especially for the split MRB with dynamic switch between PTM and PTP mode at handover could imply some issues and thus additional complexity.
        4. The security is under control in the PLMN. The "double ciphering" in service layer and in air interface is avoided.
      * …
  + Proposal for way forwards
    - Service layer as baseline:
      * Huawei,..
    - Transport layer as baseline:
      * …
    - Support both Service layer and Transport layer:
      * …
  + Decisions:
    - …
* Contribution from Philips
  + Comments and suggestions..

**Part two: Authentication and authorization**

* **Potential security requirements:** 
  + **The 5GS shall support the authentication and authorization for multicast communication service.**
* **Potential solution: sol#4**
  + **Proposal:** During CP Join, EAP based secondary authentication method in solution #4 can be used for authentication and authorization for multicast communication service
    - **Support:**
    - **Object:**
  + Decisions:
    - …

**Part three: Recommendation**

**Finalize the solution as much as possible and address the ENs**