SA3/SA3-LI joint conf call on AKMA roaming LI requirements

7th September 3:00 PM - 4:30 PM (CEST)

AKMA roaming scenarios can be structured as followed:

Case 1: UE in VPLMN and accessing an internal HPLMN AF

Case 2: UE is in VPLMN and accessing an internal VPLMN AF

Case 3: UE is in VPLMN and accessing an AF in the Data Network (Internet)

**List of Questions for discussion:**

1. For Case 1, LI requires HPLMN to provide the means to decrypt the user services, e.g., the encryption key.

Note: Apart from the encryption key, other crucial information (e.g., nonces, counters, selected cipher algorithm) in order to decrypt are also obliged to be provided. For simplicity, we just focus on the encryption key in this doc for example.

1. If the encryption key is KAF, then KAF shall be provided. **Yes or No**?
2. If the encryption key is derived from KAF, e.g. in TLS profile, then the encryption key shall be provided, KAF is not needed to be provided. **Yes or No**?
3. If the encryption key has nothing to do with KAF, e.g. KAF is only used for authentication, while the encryption key is established according to an application layer protocol, then the encryption key shall be provided, KAF is not needed to be provided. **Yes or No**?
4. For Case 2, since the AF knows everything about the encryption key, LI requirements can be met by the AF without additional requirement to the HPLMN. **Yes or No?**
5. For Case 3, since the AF is external, the HPLMN has no knowledge of what KAF is used to do, e.g. for authentication only, for integrity protection, or for deriving the encryption keys, the HPLMN even doesn’t know the encryption key (unless the encryption key is KAF itself).
6. If KAF is used to establish the encryption key, then only KAF and related information which are known to HPLMN shall be provided to VPLMN. **Yes or No**? Having in mind that the HPLMN cannot force the external AF to provide the encryption keys.
7. If AKMA/KAF is only used for authentication, similar as 1.c) above, AKMA has nothing to do with establishing keys by AF, **What is HPLMN obliged to do in this case?**