**3GPP TSG-CT WG1 Meeting #127bis-eC1-21xxxx**

**Electronic meeting, 25-29 January 2021**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **2953** | **rev** | **1** | **Current version:** | **17.1.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Collision of AKMA and NAS AKA procedure handling |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | AKMA-CT |  | ***Date:*** | 2021-01-11 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)Rel-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)* |
|  |  |
| ***Reason for change:*** | About when to derive KAKMA and A-KID at the UE, As per specified in TS 24.501, it was specified as per below yellow text:"*Upon receiving a request from upper layers to obtain AKMA Anchor Key (KAKMA) and AKMA Key Identifier (A-KID), the UE shall derive the KAKMA and the AKMA Temporary Identifier (A-TID)* ***from the KAUSF if available*** *as specified in 3GPP TS 33.535 [24A], shall further derive the A-KID from the A-TID as specified in 3GPP TS 33.535 [24A] and shall provide KAKMA and A-KID to the upper layers.*"The keyword "***from the KAUSF if available***" means whenever the UE NAS received the request from upper layers, it shall always use the current available KAUSF for the derivation of KAKMA and A-KID, regardless of any other conditions.However, in case of the collision of AKMA and EAP-AKA procedure, the current available KAUSF may not be updated yet and hence, the UE may use the outdated KAUSF for the derivation of KAKMA and A-KID which will not aligned with the network side. Typically in below scenario:1. *The UE and the network (i.e. AUSF) has shared the same KAUSF#1 after the previous successful AKA (either EAP-AKA or 5G-AKA) procedure, i.e. the current availble KAUSF at the UE is KAUSF#1.*
2. *Then, the network initiates a new EAP-AKA procedure to the UE by sending a NAS AUTHENTICATION REQUEST message including an EAP-request message. In this step, the UE does not generate the new KAUSF (Note that upon receipt of EAP-request message, it is optional for the UE to generate the new KAUSF.)*
3. *At the same time, the UE NAS receives the request from upper layers to obtain KAKMA and A-KID. As per current CT1 spec, the UE NAS shall derive KAKMA and A-KID from the current available KAUSF#1 and then provide them to upper layers for AKMA.*
4. *Hereafter, EAP-AKA was successfully performed and both the UE and the network (i.e. AUSF) will share a new KAUSF#2, i.e. the current avaible KAUSF at the UE is KAUSF#2.*
5. *Finally, the network will use KAUSF#2 to derive the KAKMA and A-KID but the UE used KAUSF#1 to derive the KAKMA and A-KID for AKMA, which caused AKMA key desynchronization between the UE and the network.*

Hence, to avoid the possible misaignment on used KAUSF to derive KAKMA and A-KID for AKMA between the UE and the network, it would propose that: during the ongoing EAP-AKA procedure, when received the request from upper layers to obtain KAKMA and A-KID, the UE shall derive KAKMA and A-KID after the completion of the ongoing EAP-AKA procedure.Even the problem may not easily happen during the 5G-AKA procedure (due to in 5G-AKA procedure, the UE will generate the new KAUSF upon recept of the NAS AUTHENTICATION REQUEST *message*), in order to provide a consistent handling for collision of AKMA and NAS AKA procedure, the above proposal can also apply to 5G-AKA procedure as well. |
|  |  |
| ***Summary of change:*** | To avoid the possible misalignment on used KAUSF to derive KAKMA and A-KID for AKMA between the UE and the network, it proposes that: during the ongoing EAP-AKA or 5G-AKA procedure, when received the request from upper layers to obtain KAKMA and A-KID, the UE shall derive KAKMA and A-KID after the completion of the ongoing EAP-AKA or 5G-AKA procedure. |
|  |  |
| ***Consequences if not approved:*** | The used KAUSF to derive KAKMA and A-KID for AKMA may be mis-aligned between the UE and the network which caused AKMA key desynchronization. |
|  |  |
| ***Clauses affected:*** | 4.21 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\* \* \* First Change \* \* \* \*

4.21 Authentication and Key Management for Applications (AKMA)

The purpose of AKMA is to provide authentication and key management to applications based on 3GPP credentials used for 5GS access as specified in 3GPP TS 33.535 [24A], which allows the UE to securely exchange data with an application server.

Upon receiving a request from upper layers to obtain AKMA Anchor Key (KAKMA) and AKMA Key Identifier (A-KID), the UE shall derive the KAKMA and the AKMA Temporary Identifier (A-TID) from the KAUSF if available as specified in 3GPP TS 33.535 [24A], shall further derive the A-KID from the A-TID as specified in 3GPP TS 33.535 [24A] and shall provide KAKMA and A-KID to the upper layers.

During an ongoing primary authentication and key agreement procedure (see subclause 5.4.1), if the UE receives a request from upper layers to obtain KAKMA and A-KID, the UE shall derive the KAKMA and A-TID after the completion of the ongoing primary authentication and key agreement procedure, shall further derive the A-KID from the A-TID as specified in 3GPP TS 33.535 [24A] and shall provide KAKMA and A-KID to the upper layers.

NOTE 1: The upper layers derive the AKMA Application Key (KAF) from KAKMA as specified in 3GPP TS 33.535 [24A].

NOTE 2: The knowledge of whether a certain application needs to use AKMA or not is application specific and is out of the scope of 3GPP.

NOTE 3: The exact method of securing the data exchange at upper layers using KAF is application specific and is out of the scope of 3GPP.

\* \* \* End of Change \* \* \* \*