**3GPP TSG-SA3 Meeting #107e *draft\_S3-221100-r2***

**e-meeting, 16 – 20 May 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | 1415 | **rev** | **1** | **Current version:** | **15.15.0** |  |
|  |
| *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 |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Clarification on SEQ usage on N32-f protection-R15 |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5GS\_Ph1-SEC |  | ***Date:*** | 2022-5-9 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-15 |
|  | *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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | According the Nonce definition for AES-GCM in clause 13.2.4.4.1, the SEQ used for the replay attack shall be securely stored and updated in the SEPPs side. If not, the SEPP may not be able to detect the replay attack or not with current SQN number. It is suggested to clarify the requirement of the SEQ in the SEPP side. |
|  |  |
| ***Summary of change:*** | Clarify that the SEQ used for the replay attack shall be securely stored and updated in the SEPPs side. |
|  |  |
| ***Consequences if not approved:*** | If SEQ is not securely stored during the implemenation, the replay attack may happen. |
|  |  |
| ***Clauses affected:*** | 13.2.4.4.1 |
|  |  |
|  | **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 \* \* \* \*

##### 13.2.4.4.1 N32-f key hierarchy

The N32-f key hierarchy is based on the N32-f master key generated during the N32-c initial handshake by TLS key export. The N32-f key hierarchy consists of two pairs of session keys and two pairs of IV salts, which are used in two different HTTP/2 sessions. In one Session the N32-c initiator acts as the HTTP client and in the second the N32-c responder acts as the client.

If the exported master secret is reused to set up multiple HTTP sessions or to set up new HTTP sessions on stream ID exhaustion, a new, unique, N32-f Context ID shall be generated to avoid key and IV re-use.

The master key shall be obtained from the TLS exporter. The export function takes 3 arguments: Label, Context, Length (in octets) of the desired output. For the N32 Master key derivation, the Label shall be the IANA registered label "EXPORTER\_3GPP\_N32\_MASTER" [89], the Context shall be "" (the empty string) and the Length shall be 64.

The N32 key derivation function N32-KDF shall be based on HKDF [62] and shall use only the HKDF-Expand function as the initial key material has been generated securely:

 N32-KDF (label, L) = HKDF-Expand (N32-f master key, "N32" || N32-Context-ID || label, L),

where

 - label is a string used for key separation,

 - L is the length of output keying material in octets.

Each run of N32-KDF (label, L) produces either one session key or one IV salt.

There are two pairs of session keys and IV salts to be derived.

NOTE: In AES-GCM re-use of one IV may reveal the integrity key (Joux’s Forbidden attack). The binding of session keys and IV salts to N32-f context IDs and labels is essential to protect against inadvertent use of the same key with a repeated IV.

The labels for the JWE keys are:

- "parallel\_request\_key"

- "parallel\_response\_key"

- "reverse\_request\_key", and

- "reverse\_response\_key".

The keys derived with labels starting parallel shall be used for request/responses in an HTTP session with the N32-c initiating SEPP acting as the client (i.e. in parallel to the N32-c connection). The keys derived with the labels starting reverse shall be used for an HTTP session with the N32-c responding SEPP acting as the client.

To generate the IV salts, the length is 8 and the labels are:

- "parallel\_request\_iv\_salt",

- "parallel\_response\_iv\_salt",

- "reverse\_request\_iv\_salt", and

- "reverse\_response\_iv\_salt".

The 96-bit nonce for AES\_GCM shall be constructed as the concatenation of the IV salt (8 octets, 64-bits) and the sequence counter, SEQ, following section 8.2.1 of NIST Special Publication 800-38D [63]:

 Nonce = IV salt || SEQ.

The sequence counter shall be a 32-bit unsigned integer that starts at zero and is incremented for each invocation of the encryption. A different sequence counter shall be maintained for each IV salt. The SEQ used for the replay attack shall be securely stored and updated in the SEPPs side.

\* \* \* End of Changes \* \* \* \*