**3GPP TSG-SA3 Meeting #115 *draft\_S3-240550-r1***

**Athens, Greece, 26 February – 1 March 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1924** | **rev** | **1** | **Current version:** | **18.4.0** |  |
|  | | | | | | | | |
| *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 the usage of N32-f context ID and N32-f message ID | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon, Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | Roaming5G | | | | |  | ***Date:*** | | | 2024-01-27 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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 can be 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:*** | | The reformattedData JSON element in the error message is defined to contain metadata with N32-f message ID and N32-f context ID. However, the usage of N32-f message ID and N32-f context ID is still not clear. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarify the usage of N32-f message ID and N32-f context ID. N32-f message ID and N32-f context ID are used to indicate that the message is the error message. N32-f message ID is also used to indicate the message in which the error occurred. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The usage of N32-f message ID and N32-f context ID is still not clear. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 13.2.4.7 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | S3-240550 | | | | | | | | |

\*\*\* BEGIN of 1st CHANGE \*\*\*

#### 13.2.4.7 Message verification by the receiving SEPP

The receiving SEPP determines that the received message is an error message generated by the Roaming Hub based on the reformattedData IE, which includes only the N32-f message ID and N32-f context ID.

If the received messages is not generated by a roaming hub:

- The receiving SEPP shall decrypt the JWE ciphertext using the shared session key and the following parameters obtained from the JWE object – Initialization Vector, Additional Authenticated Data value (clearTextEncapsulatedMessage in "aad") and JWE Authentication Tag ("tag").

- The receiving SEPP shall check the integrity and authenticity of the clearTextEncapsulatedMessage and the encrypted text by verifying the JWE Authentication Tag in the JWE object with the JWE AAD algorithm. The algorithm returns the decrypted plaintext (dataToIntegrityProtectAndCipher) only if the JWE Authentication Tag is correct.

- The receiving SEPP refers to the NF API in clearTextEncapsulatedMessage with values in the dataToIntegrityProtectAndCipher array.

- The receiving SEPP shall next verify IPX provider updates, if included, by verifying the JWS signatures added by the Roaming Intermediaries. The SEPP shall verify the JWS signature, using the corresponding raw public key or certificate that is contained in the IPX provider’s security information list obtained during parameter exchange in the related N32-c connection setup or, alternatively, has been configured for the particular peer SEPP.

- The receiving SEPP shall then check that the raw public key or certificate of the JWS signature IPX's Identity in the modifiedDataToIntegrity block matches to the IPX provider referred to in the "authorizedIPX ID" field added by the sending SEPP, based on the information given in the IPX provider security information list.

- The receiving SEPP shall check whether the modifications performed by the Roaming Intermediaries were permitted by the respective modification policies. The receiving SEPP shall use the modification policy of the cIPX obtained during parameter exchange in the related N32-c connection setup, and use the modification policy of pIPX configured within the receiving SEPP.

- If this is the case, the receiving SEPP shall apply the patches in the Operations field in order, perform plausibility checks, and create a new HTTP request according to the "patched" clearTextEncapsulatedMessage.

- The receiving SEPP shall verify that the PLMN-ID contained in the incoming N32-f message matches the PLMN-ID in the related N32-f context.

If the received message is an error message generated by a Roaming Hub:

- The receiving SEPP shall check that the raw public key or certificate of the JWS signature IPX's identity in the modifiedDataToIntegrityProtect block matches the adjacent Roaming Hub identity.

- The receiving SEPP determines the message in which the error occurred, based on the N32-f message ID.

- If the receiving SEPP determines from the error message that the Roaming Hub requires a modified request message, it can modify if allowed by the MNO's policy, and can resend the modified request message.

\*\*\* END of 2nd CHANGE \*\*\*