**3GPP TSG-CT WG4 Meeting #111-eC4-224xxx**

**E-Meeting, 18th – 26th August 2022 *Revision of C4-224311***

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **29.573** | **CR** | **0116** | **rev** | **1** | **Current version:** | **17.5.0** |  |
|  |
| *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:***  | Correction on applying modification policies |
|  |  |
| ***Source to WG:*** | Huawei |
| ***Source to TSG:*** | CT4 |
|  |  |
| ***Work item code:*** | TEI16 |  | ***Date:*** | 2022-07-30 |
|  |  |  |  |  |
| ***Category:*** | A |  | ***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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | The modificationsBlock from IPX shall be applied to the information that is only integrity protected, but the description of the modificationsBlock is related to the IE not defined in the specification.Based on the LS in C4-224033 from SA3, there is misalignment between SA3 on handling of the modification policy in the receiving SEPP. In the current definition, the JSON patch modification is applied to the original JSON request/response body, which is incorrect, it shall be applied to the DataToIntegrityProtectBlock.The SEPP forms the original JSON request / response body from the decrypted ciphertext and the decoded integrity verified "aad" block possibly modified as described above. |
|  |  |
| ***Summary of change:*** | Correct the IE name to DataToIntegrityProtectBlock;Correct the handling of the modification policy in the receiving SEPP. |
|  |  |
| ***Consequences if not approved:*** | Incorrect definition on the attribute and handling of the modification policy may cause the failure to apply the modification policy in SEPP and IPX. |
|  |  |
| ***Clauses affected:*** | 5.3.2.1, 6.2.5.2.2, 6.2.5.2.3, 6.2.5.2.10 |
|  |  |
|  | **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 contribution does not change the OpenAPI. |
|  |  |
| ***This CR's revision history:*** |  |

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

#### 5.3.2.1 General

If the negotiated security capability between the two SEPPs is PRINS, one or more HTTP/2 connections between the two SEPPs for the forwarding of JOSE protected message shall be established, which may involve IPX providers on path. The forwarding of messages over the N32-f interface involves the following steps at the sending SEPP:

1. Identification of the protection policy applicable for the API being invoked (i.e either a request/response NF service API or a subscribe/unsubscribe service API or a notification API).

2. Message reformatting as per the identified protection policy.

3. Forwarding of the reformatted message over the N32 interface.

The processing of a message received over the N32-f interface at the receiving SEPP involves the following steps.

1. Identify the N32-f context using the N32-f context Id received in the message.

2. Verify the integrity protection of the message using the keying material obtained from the TLS layer during the parameter exchange procedure for that N32-f context (see 3GPP TS 33.501 [6]). The TLS connection from which the keying material is obtained is the N32-c TLS connection used for the parameter exchange procedure.

3. Decrypt the ciphertext part of the received JWE message. Decode the "aad" part of the JWE message using BASE64URL decoding.

4. For each entry in the "modificationsBlock" of the received message:

- First verify the integity protection of that entry using the keying material applicable for the IPX that inserted that block (using the "identity" IE in the "modificationsBlock");

- Identify the modifications policy exchanged during the parameter exchange procedure with the sending SEPP if the IPX that inserted the modificationsBlock is from the sending SEPP side; else identify the modifications policy applicable for the IPX based on local configuration;

- Check if the inserted modifications are as per the identified modifications policy;

- Apply the modifications as a JSON patch in the DataToIntegrityProtectBlock (from the decoded "aad" part).

5. Form the original JSON request / response body from the decrypted ciphertext and the decoded integrity verified "aad" block possibly modified as described in step 4.

6. If the reconstructed HTTP message has a "Authorization" header, then the SEPP shall check whether the service consumer's PLMN ID is present in the Bearer token contained in the Authorization header (see 3GPP TS 29.510 [18], clause 6.3.5.2.4) and if it matches with the "Remote PLMN ID" of the N32-f context. If they do not match, the SEPP shall respond to the sending SEPP with "403 Forbidden" status code with the application specific cause set as "PLMNID\_MISMATCH".

NOTE 1: In this case, the N32-f Error Reporting procedure specified in clause 5.2.5 is not used since the processing of the complete N32-f message fails at the receiving SEPP.

NOTE 2: If the service consumer's PLMN ID is present in the reconstructed HTTP message, then the receiving SEPP compares this with the sending SEPP's PLMN ID, which is retrieved from N32f Context (see clause 5.9.3 in 3GPP TS 33.501 [6]). See the above step 6 for the receiving SEPP behaviour. If the service consumer's PLMN ID is not present, the comparison is not done.

SEPPs and IPX should support gzip coding (see IETF RFC 1952 [23]) in HTTP requests and responses and indicate so in the Accept-Encoding header, as described in clause 6.9 of 3GPP TS 29.500 [4] and clause 6.2.2.2.3.

\* \* \* Next Change \* \* \* \*

##### 6.2.5.2.2 Type: N32fReformattedReqMsg

Table 6.2.5.2.2-1: Definition of type N32fReformattedReqMsg

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| reformattedData | FlatJweJson | M | 1 | This IE shall contain the integrity protected reformatted block as well as the ciphered part of the reformatted block of the HTTP/2 request message sent between NF service producer and consumer.The SEPP shall reformat the HTTP/2 request message as:- The part of original HTTP/2 request message headers and the payload that needs to be only integrity protected is first reformatted into "DataToIntegrityProtectBlock" and then fed as input for the "aad" parameter of the FlatJweJson after subjecting to BASE64URL encoding.The part of the original HTTP/2 request message headers and payload that require integrity protection and ciphering is first reformatted into "DataToIntegrityProtectAndCipherBlock" and then fed as input for JWE ciphering and the JWE ciphered block is then BASE64URL encoded and set into the "ciphertext" parameter of the FlatJweJson.  |
| modificationsBlock | array(FlatJwsJson) | C | 1..N | This IE shall be included if the IPXes on path are allowed to apply modification policies and if they have any specific modification to be applied on the message contained in the DataToIntegrityProtectBlock. |

\* \* \* Next Change \* \* \* \*

##### 6.2.5.2.3 Type: N32fReformattedRspMsg

Table 6.2.5.2.3-1: Definition of type N32fReformattedRspMsg

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| reformattedData | FlatJweJson | M | 1 | This IE shall contain the integrity protected reformatted block as well as the ciphered part of the reformatted block of the HTTP/2 response message sent between NF service producer and consumer.The SEPP shall reformat the HTTP/2 response message as:- The part of original HTTP/2 response message headers and the payload that needs to be only integrity protected is first reformatted into "DataToIntegrityProtectBlock" and then fed as input for the "aad" parameter of the FlatJweJson after subjecting to BASE64URL encoding.- The part of the original HTTP/2 response message headers and payload that require integrity protection and ciphering is first reformatted into "DataToIntegrityProtectAndCipherBlock" and then fed as input for JWE ciphering and the JWE ciphered block is then BASE64URL encoded and set into the "ciphertext" parameter of the FlatJweJson. |
| modificationsBlock | array(FlatJwsJson) | C | 1..N | This IE shall be included if the IPXes on path are allowed to apply modification policies and if they have any specific modification to be applied on the message contained in the DataToIntegrityProtectBlock. |

\* \* \* Next Change \* \* \* \*

##### 6.2.5.2.10 Type: Modifications

Table 6.2.5.2.10-1: Definition of type Modifications

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| operations | array(PatchItem) | C | 1..N | This IE shall be included if an intermediary IPX inserts modification instructions on the JSON data carried in the "DataToIntegrityProtectBlock" part of the N32-f forwarded message. For the first modifications entry, this IE shall not be included, since the first entry is inserted by the SEPP. |
| identity | Fqdn | M | 1 | This IE shall contain the identity of the entity inserting the modifications entry. The identity shall be encoded in the form of an URI. |
| tag | string | C | 0..1 | This IE shall be present when the JWE Authentication Tag value is non-empty as specified in IETF RFC 7515 [16]. When present, this IE shall contain the BASE64URL(JWE Authentication Tag). |

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