**3GPP TSG-RAN WG3 #115-e draft R3-222413**

**21th Feb – 3rd Mar 2022 Online**

Agenda Item: 30.4

Source: Vodafone (moderator)

Title: CB: # 21\_EPSUPIP - Summary of email discussion

Document for: Approval

# Introduction

***GTW time is allocated on Wednesday 23rd February, so please provide “1st round” comments by noon (12:00) UTC on Wednesday 23rd.***

This contribution summarizes the following email discussion:

|  |
| --- |
| **CB: # 21\_EPSUPIP****- Focus on critical issues to be solved in R17 and check progress in SA3 and SA2****- Detection solutions for peer node, remote node? UE’s UPIP capability for ENDC? Further cleanup if needed.****- Capture agreements and provide TPs if agreeable**(Vodafone - moderator)Summary of offline disc [R3-222413](file:///C%3A%5CUsers%5Cpudneyc%5CAppData%5CLocal%5CTemp%5C7zOC48805A7%5CInbox%5CR3-222413.zip) |

# List of contributors

To assist in resolving issues, contributors are invited to list their email address below.

|  |  |
| --- | --- |
| Company | Email address |
| Vodafone (moderator/rapporteur) | chris.pudney@vodafone.com |
| Huawei | hanfeng3@huawei.com |
| Intel Corporation | jaemin.han@intel.com |
| Qualcomm | llopes@qti.qualcomm.com |
| Ericsson | Nianshan.shi@ericsson.com |
|  |  |

# Input Documents

The following contributions were submitted for Agenda Item 30.4:

|  |  |  |
| --- | --- | --- |
| [R3-221606](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-221606.zip) | Support for User Plane Integrity Protection support for EPC connected architectures with EN-DC capable UE\_E1AP (ZTE, China Telecom, Ericsson, Vodafone, Qualcomm, Nokia, Nokia Shanghai Bell, Huawei) | CR0678r2, TS 38.463 v16.8.0, Rel-17, Cat. B |
| [R3-221607](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-221607.zip) | Introduction of User Plane Integrity Protection in EPS (Qualcomm Incorporated, Nokia, Nokia Shanghai Bell, Huawei, ZTE, Vodafone, Ericsson) | CR1852r3, TS 36.413 v16.8.0, Rel-17, Cat. B |
| [R3-221608](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-221608.zip) | Supporting EPS User Plane Integrity Protection (Huawei, Orange, CATT, ZTE, Qualcomm Incorporated, Nokia, Nokia Shanghai Bell, Vodafone, Ericsson) | CR1663r4, TS 36.423 v16.8.0, Rel-17, Cat. B |
| [R3-221741](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-221741.zip) | (TP for S1AP BL CR on UP IP) Remaining functionality support for IP UP in EPS (Qualcomm Incorporated) | other |
| [R3-221824](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-221824.zip) | (TP for TS 36.423) Support of EPS User Plane Integrity Protection (Nokia, Nokia Shanghai Bell) | other |
| [R3-221973](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-221973.zip) | (TP for UPIP BLCR for TS 36.423) Supporting EPS User Plane Integrity Protection (Huawei, Orange, CATT) | other |
| [R3-221974](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-221974.zip) | (TP for UPIP BLCR for TS 36.413) Supporting EPS User Plane Integrity Protection (Huawei, Orange, CATT) | other |
| [R3-221975](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-221975.zip) | (TP for UPIP BLCR for TS 38.463) Supporting EPS User Plane Integrity Protection (Huawei, Orange, CATT) | other |
| [R3-222040](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-222040.zip) | Further discussion on UPIP EPC (Ericsson) | discussion |
| [R3-222197](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-222197.zip) | (TPs for TS38.401 TS36.413 TS36.423) Supporting UPIP (ZTE) | other |
| [R3-222347](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-222347.zip) | EPS User Plane Integrity Protection with non-supporting nodes (VODAFONE) | discussion |
| R3-222485 | Reply LS on LTE User Plane Integrity Protection (SA2) | LS in |

# For the Chairman’s Notes

Propose the following:

*Text to be added*

# Discussion (1st Round)

## Status from previous meetings

WID [UPIP\_SEC\_LTE-RAN-Core]: [RP-213669](https://www.3gpp.org/ftp/tsg_ran/TSG_RAN/TSGR_94e/Docs) (target: RAN #95)

*RAN3#114bis-e: Agreements:*

The UPIP policy (‘required’, ‘preferred’, or ‘not needed’) should be signalled over S1, X2 and E1 interfaces in messages related to “E-RAB establishment”.

On the S1 interface, the UPIP policy should be included in: E-RAB SETUP REQUEST, INITIAL CONTEXT SETUP REQUEST, HANDOVER REQUEST. (Please see other bullets with regard to UE CONTEXT MODIFICATION REQUEST and E-RAB MODIFY REQUEST; the transparent container in HANDOVER REQUIRED/REQUEST; and PATH SWITCH REQUEST/ACK.)

On X2 interface, the UPIP policy should be included in: HANDOVER REQUEST, SGNB ADDITION REQUEST, SGNB MODIFICATION REQUEST and (at least because of its use for RRC re-establishment in a new eNB) RETRIEVE UE CONTEXT RESPONSE

On E1 interface, the UPIP policy should be included in: BEARER CONTEXT SETUP REQUEST and BEARER CONTEXT MODIFICATION REQUEST

On the S1 interface, use the EIA 7 bit in the UE Security Capabilities IE to inform the eNB that the UE supports UPIP.

On X2, from source eNB to target eNB, use the EIA 7 bit in the UE Security Capabilities IE to inform the eNB that the UE supports UPIP. (Please see question 2 for how to signal the UE’s UPIP support from eNB to SgNB)

There is no need to signal the UE’s support of UPIP in E1-AP as the CU-CP should only request the CU-UP to enable UPIP for UE’s that support UPIP.

Add S1-AP, X2-AP, and E1-AP cause values to report the failure to implement “UPIP=required”.

Following X2 handover, on the S1 interface in the PATH SWITCH REQUEST message, the target eNB sends the UPIP policy (received from the source eNB) to the MME for verification. If any mismatch, the MME sends back the UPIP policy to the target eNB in the PATH SWITCH REQUEST ACKNOWLEDGE.

Not modify X2 interface signaling related to LTE-LTE dual connectivity.

S1, X2, and E1 signaling should be done on a per-RAB basis (and not done on the per PDN connection basis that is used by 5GC). Per-RAB signalling aligns with the CRs agreed by SA2 and CT4.

In line with (at least) the agreed SA2 and CT 4 CRs, only the UPIP policy and not the ciphering policy is sent of S1, X2 and E1 interfaces.

In line with the agreed RAN WID (and at least SA2 CRs), LTE UPIP is for the full data rate and hence we should not signal a Maximum Integrity Protected Data Rate Uplink or Downlink on S1, X2 or E1 interfaces.

There does not seem to be any SA3 requirement nor SA2 or CT 4 procedure that leads to the need to signal a change of a RAB’s UPIP policy to the eNB. Hence it is proposed to NOT add the UPIP policy to the S1-AP E-RAB MODIFY REQUEST message.

To cope with handover from a non-supporting MME to a supporting MME, SA3 have specified that “then the MME shall send an S1 CONTEXT MODIFICATION REQUEST message to inform the eNB about the correct UE EPS security capabilities”. Hence it is proposed include the updated (LTE) UE security capabilities in the S1-AP UE CONTEXT MODIFICATION REQUEST message. (already supported in TS 36.413)

BaseLine CRs endorsed in previous meeting are resubmitted as

|  |  |  |
| --- | --- | --- |
| [R3-221606](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-221606.zip) | Support for User Plane Integrity Protection support for EPC connected architectures with EN-DC capable UE\_E1AP (ZTE, China Telecom, Ericsson, Vodafone, Qualcomm, Nokia, Nokia Shanghai Bell, Huawei) | CR0678r2, TS 38.463 v16.8.0, Rel-17, Cat. B |
| [R3-221607](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-221607.zip) | Introduction of User Plane Integrity Protection in EPS (Qualcomm Incorporated, Nokia, Nokia Shanghai Bell, Huawei, ZTE, Vodafone, Ericsson) | CR1852r3, TS 36.413 v16.8.0, Rel-17, Cat. B |
| [R3-221608](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-221608.zip) | Supporting EPS User Plane Integrity Protection (Huawei, Orange, CATT, ZTE, Qualcomm Incorporated, Nokia, Nokia Shanghai Bell, Vodafone, Ericsson) | CR1663r4, TS 36.423 v16.8.0, Rel-17, Cat. B |

Open issues from the last meeting are:

1. **How source eNB knows target eNB capability to support UPIP at S1 and X2 handover;**
2. **How MeNB knows SgNB capability to support UPIP**
3. **How CU-CP knows CU-UP capability to support UPIP**
4. **How (e.g. at intra MME handover to non supporting eNB, or PDN connection establishment using NAS signalling via non -supporting eNB) MME knows whether eNB supports UPIP.**
5. **Whether to add the “UPIP policy in use” to the source to target transparent container in the S1 interface HANDOVER REQUIRED and HANDOVER REQUEST messages**
6. **(Dependent upon SA3 and SA2 response) whether and how to do the Notification of “UPIP in use” in RAN 3’s interfaces**
7. **Whether any updates are needed to the parts of TS 36.300 or TS 37.340 that are regarded as being under “RAN 3 responsibility”?**
8. **For EN-DC, signal the UE’s support/non-support of UPIP from the eNB to the SgNB by adding the (LTE) UE Security Capabilities IE to the SGNB ADDITION REQUEST and SGNB MODIFICATION REQUEST messages.**

Another issue that was mentioned in last meeting’s discussion is:

1. *How do we ensure that at (X2 and S1) handover from an eNB using UPIP with UPIP policy = “preferred” to a non-supporting eNB, the target eNB will construct an RRCConnectionReconfigurationCommand that ensures that the UE does NOT use UPIP on the target-non-supporting cell.*

## LS Responses from SA2 and SA3 to R3-221473

From our last RAN 3 meeting we sent an LS in R3-221473 to SA2 and SA3. It had two questions, both were for SA3 but only the second one was for SA2.

The SA2 response to the second question is in R3-222485 and basically leaves the decision to SA3:

***Question:*** *RAN3 has noted the functionality difference between EPS and 5GS, e.g., when UPIP policy is ‘preferred’, the NG-RAN node is required to notify if the UPIP is performed or not.*

*SA2 Answer: Thanks RAN3 for pointing out this. Since SA3 has specified UP IP policy, SA2 thinks SA3 should make the final decision on this question, i.e. whether a feedback is needed for this.*

The SA3 response is not yet available, but the SA3 email discussions (thread title: Re: [SA3#106e][3, UPIP][S3‑220039] Reply LS on LTE User Plane Integrity Protection) do appear to be converging. The rapporteur anticipates that we will soon get a reply that is similar to the latest draft, [draft\_S3-220302-r6](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_106e/Inbox/Drafts/draft_S3-220302-r6.docx). The **not yet agreed** SA3 answers to the RAN 3 questions in this draft LS are:

1. *(for SA3) In case of handover from a UPIP supporting eNB to a UPIP non-supporting eNB, would it be acceptable to SA3 if occasionally some packets over bearers with UPIP policy set to “required” are sent without integrity protection before the CN triggers the release of the bearer?*

*[SA3 answer]: SA3 prefers to avoid it since this violates the expected security policy.*

1. *(for SA3 and SA2) RAN3 has noted the functionality difference between EPS and 5GS, e.g., when UPIP policy is ‘preferred’, the NG-RAN node is required to notify if the UPIP is performed or not.*

*[SA3 answer]: In both EPS/LTE and 5GS, SA3 currently does not have any security requirement for the RAN (eNB) to notify Core Network when UP IP policy is set to ‘Preferred’. SA3 only requires that the DRBs for which the UP IP policy set to ‘Required’ is not handed over to target RAN nodes that cannot fulfil this requirement.*

Given the short timescales for this WID, and that the above answers align with the existing SA3, SA2, and CT4 Release 17 specifications for EPS UPIP, the rapporteur suggests that we start our work using the answers above.

**Q1: Do you accept the above answers, and hence that:**

1. **RAN 3 should ensure that all packets sent on a RAB that has a UPIP Policy of “UPIP=required” are integrity protected, and,**
2. **that there is no security or core network requirement for the eNB to inform the MME about the use/non-use of UPIP when UPIP=preferred?**

|  |  |  |
| --- | --- | --- |
| Company | Yes/no | Comment |
| Huawei | Yes | We can follow SA3 decisions.  |
| Intel Corporation | Yes |  |
| Qualcomm | Yes |  |
| Ericsson | Yes | The proposed way forward is fine. |
|  |  |  |
|  |  |  |

Note: Related to the second question in our LS, R3-222197 (ZTE) and R3-222040 (Ericsson) propose to remove the notifications, while R3-221974/1973 (Huawei, Orange CATT) propose, “Over S1, add the security (UPIP) results in the E-RAB MODIFICATION INDICATION message.”

## Base line CR check and small updates

### Base line CRs

The previously endorsed baseline CRs are resubmitted as:

|  |  |  |
| --- | --- | --- |
| [R3-221606](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-221606.zip) | Support for User Plane Integrity Protection support for EPC connected architectures with EN-DC capable UE\_E1AP (ZTE, China Telecom, Ericsson, Vodafone, Qualcomm, Nokia, Nokia Shanghai Bell, Huawei) | CR0678r2, TS 38.463 v16.8.0, Rel-17, Cat. B |
| [R3-221607](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-221607.zip) | Introduction of User Plane Integrity Protection in EPS (Qualcomm Incorporated, Nokia, Nokia Shanghai Bell, Huawei, ZTE, Vodafone, Ericsson) | CR1852r3, TS 36.413 v16.8.0, Rel-17, Cat. B |
| [R3-221608](file:///D%3A%5C%E4%BC%9A%E8%AE%AE%E7%A1%AC%E7%9B%98%5CTSGR3_115-e%5CDocs%5CR3-221608.zip) | Supporting EPS User Plane Integrity Protection (Huawei, Orange, CATT, ZTE, Qualcomm Incorporated, Nokia, Nokia Shanghai Bell, Vodafone, Ericsson) | CR1663r4, TS 36.423 v16.8.0, Rel-17, Cat. B |

### New Rel 17 TS for E1 interface

The Release 17 work on making the E1 interface usable by E-UTRAN and not just NG-RAN means that no release 17 version of TS 38.463 will be created. Instead a new 37 series TS will be used. The current CR in R3-221606 will need to be editorially modified (e.g. CR cover page changes) to target the new 37 series TS.

### Path Switch procedure

Our last RAN 3 meeting agreed on the following for the Path Switch procedure:

Following X2 handover, on the S1 interface in the PATH SWITCH REQUEST message, the target eNB sends the UPIP policy (received from the source eNB) to the MME for verification. If any mismatch, the MME sends back the UPIP policy to the target eNB in the PATH SWITCH REQUEST ACKNOWLEDGE.

This agreement is not captured in R3-221607 because the discussion under agenda item 8.3.1 “Handling of UE Security Capabilities” is expected to document some or all of this behaviour.

### Proposed update to BL CR in R3-222040 (Ericsson)

Amongst other proposals, this document proposes the following two updates to the SA-1P CR in R3-221448=R3-221607:

|  |  |
| --- | --- |
| *UP integrity protection not possible* | *The ~~PDU session~~ E-RAB cannot be accepted according to the required user plane integrity protection policy.* |

#### *9.2.1.xx1 Security Indication*

*This IE contains the user plane integrity protection indication which indicates the requirements on UP integrity protection for corresponding E-RABs.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *IE/Group Name* | *Presence* | *Range* | *IE type and reference* | *Semantics description* |  |  |
| *Integrity Protection Indication* | *M* |  | *ENUMERATED (required, preferred, not needed, …)* | *Indicates whether UP integrity protection shall apply, should apply or shall not apply for the concerned E-RAB.* |  |  |

### Proposed update to BL CR on E1 interface in R3-221973/1975 (Huawei, Orange, CATT)

R3-221973 gives this explanation for the Text Proposal in R3-221975:

## *2.6 E1: DRB To Modify in the Bearer Context Modification Request/Response message*

*In BLCR for E1 R3-221434, the security indication and the security results are included for the DRB to modify list in the bearer context modification request/response message.*

*For the NR PDCP, it should follow the same note described in TS 38.331 that the enable/disable the UPIP can only be performed by the DRB release, and add, but not the DRB modify procedure.*

* + *NOTE 5: Ciphering and integrity protection can be enabled or disabled for a DRB. The enabling/disabling of ciphering or integrity protection can be changed only by releasing and adding the DRB*

*Then over E1, there is no need to add the security indication/result for the DRB To Modify List / DRB Modified List in the bearer context modification procedure*

***Proposal 7: Over E1, remove the security indication/result f*rom the DRB To Modify List /** **DRB *Modified List in the bearer context modification procedure.***

### Question 2

**Q2: Do you agree:**

1. **to continue using R3-221606, 1607, and 1608 as the basis of our work in this meeting;**
2. **make the above 3 changes described in sections 5.3.4 and 5.3.5;**
3. **later in this meeting, or afterwards, convert the E1 interface CR in 38.463 into the necessary document for production of the new 37 series E1 interface specification; and**
4. **later in this meeting, or afterwards, ensure that the S1-AP CR(s) under agenda item 8.3.1 “Handling of UE Security Capabilities” enable the target eNB to send the UPIP policy (received from the source eNB) to the MME for verification. If any mismatch, the MME sends back the UPIP policy to the target eNB in the PATH SWITCH REQUEST ACKNOWLEDGE”?**

|  |  |  |
| --- | --- | --- |
| Company | Yes/no | Comment |
| Huawei | Yes with comments.  | B seems to describe two changes in section 5.3.4 and 5.3.5? if so, yes. For d), the S1AP BLCR in R3-221607 already includes the security indication in the path switch request/ack message. And the discussion in 8.3.1 including UE 4G security capabilities seems not relevant to the discussion here.  |
| Intel Corporation | Yes with comments | a) - OK with some suggestions/fixes in the below row (that I spotted so far). b) - E///'s editorial is OK, but HW's P7 needs further check. For modification of security policy, as part of CB: # 8\_SecPolicy\_E1, we are trying to cover abnormal behaviour due to release/add of DRBs requirement from 38.331. If here in EPS-UPIP there is no case to "modify" UPIP policy toward the same CU-UP, then we are fine with HW's proposal. But if this is not the case, then we can add the similar abnormal text onto E1 BL CR.  |
| **In R3-221606 (E1)**- In 8.3.1.2, * For each DRB for which the *Security Indication* IE is included in the *DRB To Setup List E-UTRAN* IE of the BEARER CONTEXT SETUP REQUEST message, and the *Integrity Protection Indication* IE is set to "preferred", then the gNB-CU-UP should, if supported, perform user plane integrity protection for the concerned DRB and notify whether it performed the user plane integrity protection by including the *Integrity Protection Result* IE, in the *DRB Setup List E-UTRAN* IE of the BEARER CONTEXT SETUP RESPONSE message.
* For each DRB for which the *Security Indication* IE is included in the *DRB To Setup List E-UTRAN* IE of the BEARER CONTEXT SETUP REQUEST message, and the *Integrity Protection Indication* IE is set to "required", then the gNB-CU-UP shall, if supported, perform user plane integrity protection, for the concerned PDU Session. If the gNB-CU-UP cannot perform the user plane integrity protection, it shall reject the setup of the DRB with an appropriate cause value.
* For each DRB for which the *Security Indication* IE is included in the *DRB To Setup List E-UTRAN* IE of the BEARER CONTEXT SETUP REQUEST message, and the *Integrity Protection Indication* IE is set to "not needed", then the gNB-CU-UP shall not perform user plane integrity protection for the concerned DRB;

- In 8.3.2.2, * For each DRB for which the *Security Indication* IE is included in the *DRB To Setup Modification List E-UTRAN* IE of the BEARER CONTEXT MODIFICATION REQUEST message, and the *Integrity Protection Indication* IE is set to "preferred", then the gNB-CU-UP should, if supported, perform user plane integrity protection, for the concerned DRB and notify whether it performed the user plane integrity protection by including the *Integrity Protection Result* IE in the *DRB To Modify List E-UTRAN* IE of the BEARER CONTEXT MODIFICATION RESPONSE message.
* For each DRB for which the *Security Indication* IE is included in the *DRB To Setup Modification List E-UTRAN* IE of the BEARER CONTEXT MODIFICATION REQUEST message, and the *Integrity Protection Indication* IE is set to "required", then the gNB-CU-UP shall, if supported, perform user plane integrity protection, for the concerned DRB. If the gNB-CU-UP cannot perform the user plane integrity protection, it shall reject the setup of the DRB with an appropriate cause value.
* For each DRB for which the Security Indication IE is included in the *DRB To Setup Modification List E-UTRAN* IE or in the *DRB Setup Modification List E-UTRAN* IE of the BEARER CONTEXT MODIFICATION REQUEST message and the *Integrity Protection Indication* IE is set to "not needed", then the gNB-CU-UP shall not perform user plane integrity protection for the concerned DRB;

**In R3-221608 (X2)**- in 8.2.1.2For each E-RAB for which the *Security Indication* IE is included in the *E-RAB To Be Setup Item IEs* IE of the HANDOVER REQUEST message, and the EIA7 bit in the *Integrity Protection Algorithms* IE contained in *UE Security Capabilities* IE is set to '1': - if the *Integrity Protection Indication* IE is set to "required", the eNB shall, if supported, perform user plane integrity protection for the concerned E-RAB as specified in TS 33.401 [15].- if the *Integrity Protection Indication* IE is set to "preferred", the eNB should perform user plane integrity protection for the concerned E-RAB as specified in TS 33.401 [15].- if the *Integrity Protection Indication* IE is set to "not needed", the eNB shall not perform user plane integrity protection for the concerned E-RAB.  |
| Qualcomm | Yes with comments | Basically agree with Huawei’s comments |
| Ericsson |  | 1. also think it meant the changes in 5.3.4 (Ericsson paper) and 5.3.5 (Huawei paper). Updated b) accordingly. Agree the proposed three changes.
 |
|  |  |  |
|  |  |  |

## How the source eNB knows the target eNB’s UPIP capability at inter-MME S1 handover

Two input documents suggest getting a supporting eNB to send a new IE within the source to target transparent container (whose absence the source eNB can use to determine that the target eNB does not support UPIP):

**R3-221741 (Qualcomm):**

*Proposal 2: For remote RAN nodes, enable detection of support by requiring a supporting eNB to provide the Security Result to the source as part of the handover preparation signalling; OAM is also not precluded.*

**R3-222347 (Vodafone)**

*Proposal 1: For S1 handover, a new IE (that indicates whether the bearer is UPIP protected or not) is added (per EPS bearer) into the target to source transparent container in the S1-AP Handover Request Acknowledge and Handover Command messages, and the source eNB is mandated to cancel handovers for when a “UPIP=required” policy cannot be maintained.*

While **R3-222040 (Ericsson)** proposes that this discussion is related to the agenda item 31.2.4 discussion in TEI 17 “Support exchange of protocol support at target RAN node for NG handover”.

An initial review of the discussion documents under agenda item 31.2.4 (R3-221738 (Qualcomm, Vodafone) and R3-221954 (Huawei, China Unicom, China Telecom) and R3-222058 (Ericsson)) indicates that some of the proposals expect that at least the MME is upgraded (e.g. because the current S1-AP Handover Failure message does not carry a “target to source transparent container”), while (subject to final SA3 confirmation) the requirements on UPIP need to cover the case of a non-supporting target MME and non-supporting eNB.

Note that 3GPP has received requests from 5GAA to support inter-PLMN handovers and that PLMN boundaries could lead to different UPIP support levels in the MMEs.

**Q3: For S1 handover, do you agree to require a supporting target eNB to provide the Security Result to the source eNB in the target to source transparent container? If not please explain how the situation of non-supporting MME and non-supporting eNB is handled for the case of a UPIP policy of “required”.**

|  |  |  |
| --- | --- | --- |
| Company | Yes/no | Comment |
| Huawei | To be discussed at AI 31.2.4 | We would prefer this can be discussed in AI 31.2.4 (CB#16), so as to have a general solution for all potential new R17 features for S1/NG based handover. For this approach, we need to consider if the legacy eNB will accept E-RABs with the “required” UPIP policy, after the full configuration.  |
| Intel Corporation | Yes |  |
| Qualcomm | Yes |  |
| Ericsson |  | The conclusion from the RACS discussion (AI 31.2.4) should apply.The scenarios where neither RAN nor CN in a neighbouring “network portion” has upgraded with a certain feature is rare. A minimum support of features is necessary to be able to rely on a certain automatism in the network. If that is not given, OAM is still an option. |

## How the originating node knows the remote node’s UPIP capability on direct interfaces.

This includes the situations of:

1. S1 interface E-RAB SETUP REQUEST, INITIAL CONTEXT SETUP REQUEST and HANDOVER REQUEST.
2. X2 interface HANDOVER REQUEST and RETRIEVE UE CONTEXT RESPONSE
3. X2 interface SGNB ADDITION REQUEST and SGNB MODIFICATION REQUEST
4. E1 interface BEARER CONTEXT SETUP REQUEST and BEARER CONTEXT MODIFICATION REQUEST

**R3-221741 (Qualcomm)** indicates that there are at least four different options:

1. Exchange of capability support at interface setup / configuration update
2. Detection via explicit IE exchange (i.e. the security result in a response message)
3. Detection via criticality (rejection pointing to the specific IE)
4. OAM

There seem to be different views on which approach to take:

**R3-221741 (Qualcomm)** proposes:

*Proposal 1: Enable detection of support of eNB support by the MME via criticality settings; OAM is also not precluded.*

*Proposal 3: In order to maintain consistency between detection of support between eNBs, enable also detection of support in X2 by requiring a supporting eNB to provide the Security Result to the source as part of the handover preparation signalling; OAM is also not precluded.*

**R3-221824 (Nokia)** proposes the use of S1/X2 Setup Request:

*Proposal 2: eNBs to exchange their feature support to MME.*

*Proposal 3: eNBs to exchange their feature support to neighbour eNBs.*

**R3-222040 (Ericsson)** proposes:

*Proposal 1: In X2AP BL CR, use Assigned Criticality “reject” for the Security Indication IE*

*Proposal 2: In E1AP BL CR, use Assigned Criticality “reject” for the Security Indication IE*

**R3-222197 (ZTE)** proposes:

*Proposal 1: RAN node aware target‘s capability to support UPIP at S1/X2 can be supported via OAM.*

*R3-221973 (Huawei) proposes:*

*Proposal 5: RAN3 to discuss the above three options, based on the reply LS from SA2/SA3.*

With the exception of OAM (which causes issues for multi-vendor and/or inter-PLMN operation) there do not appear to be decisive arguments for or against the options. However, we do need to solve this issue to meet the requirements from SA2 and SA3. From the dialogue at previous meetings it seems that the ‘critcality=reject’ has been used in previous similar situations, so the moderator suggests that we see if this can be adopted as the way forward.

**Q4: Do you accept to use an Assigned Criticality of “reject” for the UPIP Policy as the mechanism to detect UPIP supporting/non-supporting nodes for the following situations:**

1. **S1 interface E-RAB SETUP REQUEST, INITIAL CONTEXT SETUP REQUEST and HANDOVER REQUEST;**
2. **X2 interface HANDOVER REQUEST and RETRIEVE UE CONTEXT RESPONSE;**
3. **X2 interface SGNB ADDITION REQUEST and SGNB MODIFICATION REQUEST; and**
4. **E1 interface BEARER CONTEXT SETUP REQUEST and BEARER CONTEXT MODIFICATION REQUEST.**

|  |  |  |
| --- | --- | --- |
| Company | Yes/no | Comment |
| Huawei | Yes | We can have a simple solution for all direct interfaces (the same as RACS).  |
| Intel Corporation | Yes |  |
| Qualcomm | Yes with slight comment | As we mentioned, we might want to align inter-gNB handling regardless of direct or indirect connection. However no strong view. |
| Ericsson | Yes | The Assigned Criticality should be “reject” for the UPIP Policy. It is so important so that if the receiving Node is not understanding the IE or support the feature, the procedure should fail. |

## Turning off UPIP at handover to a non-supporting eNB

When the UPIP policy is “UPIP=preferred” and UPIP is in use on the source eNB, it is essential that a UPIP-non-supporting target eNB configures the new radio resource so that the UE does not expect the target eNB to be using UPIP.

This is important for the both the case that the target eNB is “pre-release 15” (and hence does not understand TS 36.331 HandoverPreparationInformation describing EN-DC) and the case that the target eNB is Rel 15/16 (and does understand about EN-DC).

In section 4 of R3-222347 (Vodafone) there is some analysis of the situation. If the analysis is correct, it seems likely that a pre-Rel 15 (non-supporting) target eNB would detect that descriptions of some EPS bearers were missing and hence provide a ‘full radio configuration’ to the UE; and a Rel 15/16 (non-supporting) target eNB would understand that UPIP was in use and hence provide sufficient radio configuration to the UE to turn off UPIP.

Companies are invited to review section 4 of R3-222347 and/or perform their own analysis.

**Question 5: do you agree that legacy target eNBs will disable UPIP in the UE at S1/X2 handover from a source eNB that was using UPIP (with UPIP policy=preferred).**

|  |  |  |
| --- | --- | --- |
| Company | Yes/no | Comment |
| Huawei | Yes | We understand that if the legacy target eNB does not understand the UPIP info in the source RRC configuration, then it will trigger full configuration. So nothing is broken.  |
| Intel Corporation | Yes | We agree with the analysis from the moderator. |
| Qualcomm | Yes | This is also our understanding but would like to hear infrastructure vendor’s views.  |
| Ericsson |  | A legacy node which does not support feature X will not support feature X. |

## How should the MeNB inform the SgNB that the UE supports UPIP?

In the previous RAN 3 meeting there was discussion – but no agreement – on the proposal that “*For EN-DC, signal the UE’s support/non-support of UPIP from the eNB to the SgNB by adding the (LTE) UE Security Capabilities IE to the SGNB ADDITION REQUEST and SGNB MODIFICATION REQUEST messages”*

**R3-221973 (Huawei, Orange, CATT)** proposes that a new dedicated IE is used for this purpose. This aligns with the current BL CR in R3-221608.

**Question 6: do you agree to use a new dedicated IE in the SGNB ADDITION REQUEST and SGNB MODIFICATION REQUEST messages to inform the SgNB that the UE supports EIA7 (EPS-UPIP)?**

|  |  |  |
| --- | --- | --- |
| Company | Yes/no | Comment |
| Huawei | Yes | SA3 has completed R17 work, we should do alignment. |
| Intel Corporation | Yes (but no strong view) | We tend to share the same view that we don't have to supply unnecessary algorithms. |
| Qualcomm | Yes |  |
| Ericsson | No | Do no see the need for a new dedicated IE as in BL CR with FFS.Instead, we shall use the “*UE Security Capabilities”. It is* more future proof and align to how we handle the security capability. |

## Whether to add the “UPIP policy in use” to the source to target transparent container in the S1 interface HANDOVER REQUIRED and HANDOVER REQUEST messages

The main benefit of this seems to be for the situation of handover to a UPIP-supporting eNB that is connected to a non-supporting MME, and, UPIP is in use at the source eNB with a UPIP policy of “preferred”. While the benefits of doing this may be low, it is required by the SA3 specification TS 33.401 and it seems easy to specify on the S1 interface.

**Question 7: do you agree to add the “UPIP policy in use” to the source to target transparent container in the S1 interface HANDOVER REQUIRED and HANDOVER REQUEST messages?**

|  |  |  |
| --- | --- | --- |
| Company | Yes/no | Comment |
| Huawei | Yes | Here the “UPIP policy in use” should be updated to “Security Indication”, which is already included in the S1AP BLCR. We can simply follow SA3 specification.  |
| Intel Corporation | Yes |  |
| Qualcomm | Yes |  |
| Ericsson |  | SA3 states that “the source eNB shall also send the UE’s UP integrity protection policy if received from the source MME to the target eNB in a source-to-target container.”So the received UPIP Policy (is this what” UPIP policy in use” means) is sent from S to T ran. |

## Do we need any update to TS 38.401 or TS 36.401?

**R3-222197 (ZTE)** proposes an update to TS 38.401. However, the existing TS 38.401 does not seem to refer to TS 33.501 (or TS 33.401) for any UE<->network security issues, and, the changes are targeted at section 7 of TS 38.401 which is for NG-RAN functions.

Text proposal for TS 38.401 from R3-222197:

## *7.X Support for User Plane Integrity Protection support for EPC connected architectures with EN-DC capable UE*

*The eNB-UP supports the user plane integrity protection functionality as specified in TS 33.401 [x].*

Extract of TS 38.401 contents list:

7 NG-RAN functions description 19

7.0 General 19

7.1 NG-RAN sharing 19

7.2 Remote Interference Management 19

7.3 Cross-Link Interference Management 20

7.4 Support for Non-Public Networks 20

7.5 RACH Optimisation Function 20

7.6 Positioning

The rapporteur investigated **whether updates to TS 36.401 might be needed.** This seems unnecessary as its text (below) already encompasses UPIP (although the text could be editorially improved to e.g. “… protected against alteration by a non-authorized third-party ~~from alteration”~~):

Extract from TS 36.401:

### *7.2.2 Radio channel ciphering and deciphering*

*This function is a pure computation function whereby the radio transmitted data can be protected against a non-authorized third-party. Ciphering and deciphering may be based on the usage of a session-dependent key, derived through signalling and/or session dependent information.*

### *7.2.3 Integrity protection*

*This function is a pure computation function whereby the transmitted data can be protected against a non-authorized third-party from alteration.*

**Q8: are any updates needed for EPS UPIP in TS 38.401 or TS 36.401?**

|  |  |  |
| --- | --- | --- |
| Company | Yes/no | Comment |
| Huawei | No | No need for TS 38.401, since the EPS UPIP is related to eNB architecture. And agree with the moderator that no need for TS 36.401.  |
| Intel Corporation | No | We agree with the moderator's understanding.  |
| Qualcomm | No | At least this does not seem essential  |
| Ericsson | No | Do not see the clear need either. |
|  |  |  |
|  |  |  |

# Topics not handled this meeting:

Owing to the limitation on the number of questions per ComeBack the following topic(s) were not treated in this meeting.

1. In R3-221973 (Huawei, Orange , CATT) proposal 6

*Proposal 6 - Over S1/X2, specify the target eNB’s behaviour in case the UPIP policy is not received while receiving the UEs UPIP capability.*

However, this proposal was discussed in the previous RAN 3 meeting and did not attract support.

# Discussion (2nd round), if needed

TBD

# Conclusions, Recommendations

TBD