Rapporteur's minutes for UPIP in SA3 98bis-e

Date: 17/04/2020 @ 12:00 UK Time (BST)

Version: 4

Author: Tim Evans, Vodafone (rapporteur of UPIP study item)

# Summary:

|  |  |  |
| --- | --- | --- |
| Doc no. | Title | Current status |
| S3-200611 | UPIP-Update for solution#10 | No Comments |
| S3-200631 | pCR to TR 33.853 (UPIP): addition of new solution - used NR PDCP for LTE | Under discussion |
| S3-200745 | UPIP: pCR for new solution of UP IP in EPS | Under discussion |
| S3-200746 | UPIP: pCR for new solution for option 5 | No Comments |
| S3-200761 | Using existing algorithm IEs to indicate support UP IP with an eNB | Under discussion |
| S3-200699 | Reduced overhead for UP IP for 5G RAN\_conclusion | Under discussion |
| S3-200700 | Conclusion to Key Issue #5 | Under discussion |
| S3-200768 | Proposed conclusion for Key Issue #6 in TR 33.853 | Under discussion |
| S3-200632 | draft WID - Normative changes for UPIP | No Comments |
| S3-200633 | CR to 33.501 - Update to User Plane Integrity Protection | Under discussion |
| S3-200696 | UP integrity protection for UP Signalling messages | Under Discussion |
| S3-200697 | Integrity protection of DNS messages | Under Discussion |
| S3-200618 | Mandatory User Plane Integrity for 5G | Final Status**Noted** |
| S3-200643 | UPIP Way Forward Discussion | Under Discussion |
| S3-200695 | Proposed solution for UP IP issues in GSMA LS | Final Status**Noted** |
| S3-200737 | Discussion on endorsement for UP IP | Under Discussion |
| S3-200766 | On the GSMA LS on UP IP | Under Discussion |
| S3-200767 | Proposed solution for UP IP issues in GSMA LS | Under Discussion |
| S3-200629 | pCR to TR 33.853 move of network options from introduction to section 4 | Under Discussion |
| S3-200635 | Cover sheet for TR 33.853 for Information | No Comments |
| S3-200639 | pCR to 33.853 (UPIP) - Correction to Key Issue 5 | No Comments |
| S3-200760 | Interworking between EPS and 5GS when UP IP is supported in EPS | No Comments |
| S3-200636 | minutes of UPIP confcall #1 on 2 April 2020 | Propose to Note this document |
| S3-200637 | minutes of confcall 2 on UPIP held 3 April 2020 | Propose to Note this document |
| S3-200634 | LS to RAN3 and CT1 on Updated User Plane Integrity Protection advice | Under Discussion |
| S3-200738 | Draft LS on UP IP | No Comments |
| S3-200630 | pCR to TR33.853 (UPIP) - Addition of conclusions to section 7.2 | Final Status**Withdrawn** |
| S3-200638 | Discussion document on the approval of TR33.853 | Final Status**Withdrawn** |

# S3-200611 UPIP-Update for solution#10 *Apple*

**Current Status: No Comments**

**Blockers: None**

**Expected Status at end of meeting (unless there are further comments): Approved**

# S3-200631 pCR to TR 33.853 (UPIP): addition of new solution - used NR PDCP for LTE *VODAFONE Group Plc*

**[email] China Mobile (vice Chair):** Note as it is for R17

**[email] Vodafone:** Do not accept China Mobiles argument as: This contribution is for the study document which covers actions on this topic over several releases. Putting solutions into the study document so that they can be correctly recorded and evaluated is important (for all valid solutions not just mine). The evaluation section is FFS in this pCR and you can input any evaluation you like in the next meeting. If you would like to add a editors note to the pCR regarding the release then say so.. Just saying note the document is not acceptable as it will prevent progress on the topic.

**[email] China Mobile (vice Chair):** Claimed cannot be accepted unless for R16

**[email] VF:** Asked the chair for clarification

**[email] China Mobile (Vice Chair):** stated - If we check the meeting agenda(S3-200600), The meeting objectives are shown there:

- Rel-16 exceptions

- Progress work on FS\_UP\_IP\_Sec in particular for option 2

I think it is very clear the target of this meeting is to push Rel16 work finished as much as possible and mainly focus on Stand-alone option.

**[email] Vodafone (rapporteur):** As you point out - it says mainly focus on NOT only focus on - so I do not agree to your objection on these grounds.

**[email] Futurewei:** Let me try to propose on suggestion to see if SA3 can get this contribution agreed:

* Remove any reference to R17 and instead made it an assumption about the availability of CP-UP split of E-UTRAN for the architectural option mentioned in the contribution.
* Since this is a study, it would be OK to make certain assumptions and base the solution on those assumptions. Of course, certain assumptions come with certain impacts (i.e. UE, core, RAN) and we just need to capture those as well.

**[email] Qualcomm:** Qualcomm proposes that this document is noted as the proposed solution is not viable for the following reasons:

- UP IP (or even UP encryption) capability is not tied to a specific PDCP version (i.e., LTE PDCP or NR PDCP) and it should be independent of PDCP version used

- Whether a UE is able to support UP IP over specific RAT is dependent on the capability of the UE (e.g., whether it has the necessary hardware resources over a specific RAT) and not whether it supports NR PDCP or not

- The existing UE security capability (e.g., supported security algorithms) negotiation is on a RAT basis (e.g., E-UTRA vs NR) and this solution jeopardizes this principle

**[email] China Mobile (Vice Chair):** The argument could not cover what we really need in this meeting. The meeting is used to make sure we finalize our work in release 16 and allow enough time for stage 3 work as well. The debating does not take any more time for other agenda item, but will take time and impact discussion on other topics in UP IP item. We still have many important contributions need to be discussed and concluded, such as how to make full rate UP IP, what is the way forward, what conclusion we need and any other contributions which helps to finalize Rel.16 work. Let’s concentrate on those topic, make progress of whole study item and not waste time on debating in this contribution. China Mobile still object this contribution in this meeting. You can bring the contribution back in future meeting if you like.

**[email] Vodafone:** It seems to me that the points you make belong in the evaluation of this solution, rather than using them as reasons not to mention the solution at all.

**[email] Vodafone (CDP):** Qualcomm said "UP IP (or even UP encryption) capability is not tied to a specific PDCP version (i.e., LTE PDCP or NR PDCP) and it should be independent of PDCP version used"

[CDP: Vodafone says this does not align with TS 24.301, see clause 9.9.3.53 (copied below) coupled with the fact that AS encryption and AS integrity protection are implemented in PDCP layer.].

- Qualcomm said "Whether a UE is able to support UP IP over specific RAT is dependent on the capability of the UE (e.g., whether it has the necessary hardware resources over a specific RAT) and not whether it supports NR PDCP or not"

[CDP (Vodafone): yes, but a UE that supports NR PDCP currently supports NR. And that type of UE is likely to support option 2 and hence should (in our view) support full rate UP IP. Hence the UE can reasonably be developed to use that full rate UP IP over LTE. When a UE is using NR PDCP with NR/LTE dual connectivity, functionality below the PDCP layer determines whether a packet is sent (or received) on LTE or NR. ]

- Qualcomm said "The existing UE security capability (e.g., supported security algorithms) negotiation is on a RAT basis (e.g., E-UTRA vs NR) and this solution jeopardizes this principle"

[CDP (Vodafone): this statement is incorrect. The radio functionality below PDCP layer decides whether a packet encrypted with NR PDCP is sent over LTE or NR radio. The NR control plane decides whether to use LTE or NR PDCP on a per EPS bearer basis. It is perfectly feasible to use LTE PDCP and route all packets over NR (option 3 with the UE in good NR coverage); or to use NR PDCP and route all packets over LTE (option 3x and the UE moves out of NR coverage)]

**[email] Qualcomm:** Response to bullet 1) I think you misinterpreted the above comment. The point of the above comment is that UP IP is a UE (and network) capability as opposed to security algorithms selection. For example, if UE supports UP IP for LTE, it can be done using LTE PDCP. There’s no restriction in LTE PDCP that it cannot support UP IP. Note that for Rel-10 relay, full-rate UP IP is supported using LTE PDCP. Similarly, NR PDCP doesn’t automatically mean full-rate support of UP IP. Qualcomm would like to keep this principle when UP IP over eUTRA is specified.

Response to Bullet 2) I think you are making specific assumptions about UE architecture. We want to reiterate that needed resources for IP (or encryption), esp. when performed in hardware as is often the case, can be RAT (eUTRA or NR) dependent and not specific version of PDCP used.

Response to Bullet 3) Again, I think you are making specific UE implementation assumptions , which is not necessarily the case in all implementations. I do agree that above is one possible way to implement (highly dependent on UE internal design). We think it is important to maintain the flexibility to negotiate UP IP on a RAT basis rather than based on PDCP basis when we introduce UP IP over eUTRA. This is the reason why the NR security algorithms use different code points compared to eUTRA algorithms. This is the point of my above comment.

Qualcomm still requests that this contribution be noted for this meeting.

**[email] CableLabs:** We support this contribution to be approved and included in the TR for further evaluation. To address Anand’s specific technical comments, would it help to add an editor note (e.g., see below) in the evaluation section ?

"Editor Notes: Evaluation of its impact on existing UE security architecture is ffs."

**[email] Qualcomm:** Unfortunately, no it does not help as there are other issues with the solution. Also, the issue is not about existing UE security arch but rather allowing flexibility for UE vendors to design an internal arch as they see fit. Also, we think there are other fundamental technical issues with the proposed solution.

**Current Status: under discussion**

**Blockers: China Mobile, Qualcomm, Spreadtrum**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200745 UPIP: pCR for new solution of UP IP in EPS Ericsson

**[email] China Mobile (Vice Chair):** The contribution needs to be updated with clear evaluation of backward capability on both UE and network side. It does not work when legacy UE wants to transfer data if MME set UP IP as required. Furthermore, as the solutions indicates that policy may from HSS, so the impact of HSS should be shown in evaluation part.

**[email] Futurewei:** I agree with China Mobile, there are big impact to legacy UE and legacy network and they should be clearly stated.

**[email] Ericsson:** I have revised the document in S3-200745 into r1 (new text is yellow marked), and uploaded it. I have added that there is impact on HSS in the evaluation clause, and also added a new editor note to the evaluation clause. You are welcome to revise the editor note further if you think this is necessary.

**[email] China Mobile (Vice Chair):** I’m glad to see the revision. I have comment on the editor’s note. It does not an evaluation. So I’d like to change it into main body text. I have revised as r2 and upload it.

**[email] Ericsson:** The intention with the proposed solution for the study, was to be able to study and update the solution continuously in Rel-17 timeframe for the next upcoming SA3 meetings. The solution is not intended for Rel-16. Would a way forward be to remove the evaluation completely from S3-200745 ? And we could also add an editor note that the solution is not complete and is intended to be studied in Rel-17?

**[email] Huawei:** I think the change on version r2 provided by CMCC makes sense. Indeed the impact because of different releases need to be considered.

**[email] Chna Mobile (Vice Chair):** Although I’m fine with your intention. I’d like to point out the current TR version 0.7.0 is marked as R16 still. So I treat this solution for R16 currently and it would be better to give an evaluation part here. What is more, when you update solution in future, I’m happy to see that corresponding evaluation text are updated at the same time.

**Current Status: Under Discussion**

**Blockers: None**

**Expected Status at end of meeting (unless there are further comments): Approved**

# S3-200746 UPIP: pCR for new solution for option 5 Ericsson

**[email] Qualcomm:** The solution states the following:‘This new spare bit would need to be signalled from the AMF to the RAN nodes and therefore mapped to a new information element on N2 interface.’ Given it is going in a new IE in the N2 won’t there also need to be changes on the Xn interface to send the ‘new spare bit’ between RAN nodes. Could we modify the solution to either capture this (as FFS in an editor’s note would be OK) or please explain if I have got this wrong.

**[email] Ericsson:** Yes, you are right that the Xn interface is impacted as well. I have made an update in r1 and added the document to the Inbox. The new text is colored in yellow. I added a new sentence about Xn interface and also an editor note for potentially further impacted network interfaces. You are welcome to update/modify if you think its needed.

**[email] Apple:** This solution looks familiar, since there is solution #8 in the current TR33.853v070. May I ask what is the main gap between 746 and the current solution #8?

**[email] Ericsson:** Solution #8 proposes to use one of the bits that is used to indicate support of an EEA or EIA algorithm in 5G UE Security Capability IE, that is currently not used. But the solution in S3-200746 proposes instead to take one of the spare bits in octet 7 in 5G UE Security Capability IE which has not yet been allocated to any purpose.

**[email] Qualcomm:** The changes are good for me.

**Current Status: Under Discussion**

**Blockers: None**

**Expected Status at end of meeting (unless there are further comments): Approved**

# S3-200761 Using existing algorithm IEs to indicate support UP IP with an eNB Qualcomm Incorporated

**[email] China Mobile (Vice Chair):** The evaluation part shall be updated. Current impact is not correct, as changing algorithm indication may cause unexpected result on legacy eNB and MME based on implementation. Some MMEs may reject UE using undefined EIA algorithm from security perspective and send warning to OSS.

**[email] Vodafone (Rapporteur):** Please update the document and place it in the drafts folder.

**[email] China Mobile (Vice Chair):** I think it is better to leave the update to contributor as he/she needs to collect all opinions from others and make response.

**[email] Qualcomm:** If an MME behaviour (and similarly eNB) rejected the UE because it set a bit to say that the UE supported an EIA algorithm that the MME did not support, then it would be impossible to add new algorithms in the UE before all networks had been upgraded.

Rejecting this would be incorrect behaviour of the MME. If you look in TS 24.301 clauses 9.9.3.34 and 9.9.3.36, you can see that the UE using a value of 1 for EIA4 to EIA7 is already specified. Hence an MME should not reject the UE just because the UE set that bit to 1. For these reasons, we do not believe that this is an issue.

**[email] DoCoMo:** I support QC’s view here

**Current Status: Under discussion**

**Blockers: China Mobile**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200699 Reduced overhead for UP IP for 5G RAN\_conclusion Philips International B.V.

**[email] China Mobile (vice Chair):** The contribution should be noted. The recommendation that solution 4 is on the normative work is not plausible, as solution 4 requires the modification on MAC layer which is non backward capable. Moreover, solution 4 actually has no benefit. It could not reduce the overhead when computing cryptographic CRC, as each packet in the MAC layer has to make a HAMC or Encryption computation.

**[email] Vodafone:** I think the “zero overhead” claim for solution 4 refers to the bandwidth overhead, not the computational overhead.

**[email] China Mobile (vice Chair):** Thanks for your clarification. But the non-backward capable issue is still there.

**[email] Philips:** Minpeng, You state that you don’t agree to the proposal in S3-200699 because of backwards compatibility issue. However, since every UE and gNB is assumed to support PDCP based integrity protection, the idea is that if a UE or gNB does not support this new mechanism for integrity protection it can simply fall back to PDCP based integrity protection, i.e. with reduced data rates due to the additional computational and message overhead of PDCP based integrity protection (as described in solution#4) but still functional. We can reuse/extend existing capability negotiation mechanisms for this, so this should not be a major issue. I hope this clarification is sufficient for you to retract your objection. If you have some additional concerns please share them with us.

**[email] Nokia:** S3-200699 should be noted, this pCR cannot be agreed. This pCR is indirectly endorsing Solution #4 “ It is further concluded that, in case further analysis in RAN/CT shows that the overhead caused by mandating full data rate user plane integrity protection based on the existing PDCP layer integrity protection mechanism has significant impact on the data rates or on UE complexity, then for Option 2 an additional mechanism based on solution #4 to enable user plane integrity protection in a more efficient manner will be specified during normative work. “

Solution#4 is to use a cryptographic CRC at PHY layer, Instead of adding MAC-I to PDCP PDUs. But there are more fundamental changes at RRC, MAC, PHY layers, I am not sure this is even possible with current protocol processing.

**[email] Spreadtrum:** Spreadtrum would support Nokia that S3-200699 should be noted. Besides the comments from Nokia, we have the following additional comments:

1. Two different mechanisms for UPIP mean that there will be two kinds of implementations on both UE and RAN, which will increase the complexity of the system.

2. We have concerns about the following statements in solution 4, which may increase the security risk since DU may not locate in a secure enough environment:

Since the negotiation of the application of this solution is done in the PDCP layer, but the application itself in the DU, the F1-C interface is extended with one or more new messages to supply the DU with the required information for the integrity protection of this solution.

**[email] Chaina Mobile (Vice Chair):** I’m fine with the clarification from Walter. However I still have concern on the conclusion. Currently PDCP layer IP is performed per DRB (which is corresponding with PDU session). However, my RAN colleague told me that DRB is invisible for MAC layer. It's not clear how to perform per DRB integrity protection if IP is done in MAC. Our purpose is to make integrity protection can be made up to full rate, but it does not mean integrity protection are mandatory used for all kinds of UP data. That is totally different. One more comment is the solution may bring some impact on the multiplexing function for MAC layer, which need to be evaluated by RAN2. So it needs to send LS to RAN2 to evaluate its impact on RAN side before choosing this solution as conclusion.

**[email] Philips:** Since you all had some technical comments on solution#4, let me try to address these one by one:

a) Comment: Solution#4 uses cryptographic CRC at PHY layer instead of adding MAC-I to PDCP PDUs. This requires fundamental changes at RRC, MAC, PHY layers, I am not sure this is even possible with current protocol processing.

Response: Yes, we acknowledge that some changes would need to be made at the PHY layers. And as mentioned in S3-200699, the time left for release 16 is probably too limited to finish this for release 16, so we would be looking at release 17 for this. The outcome and the recommendations of the FS\_UP\_IP study in TR 33.853 does not have to be limited to release 16 only and can also propose normative work for later releases. In fact, given the concerns raised by several companies during SA/RAN plenary about the overhead of the current PDCP based integrity protection mechanism, it could help to make mandatory full data rate integrity protection for all UEs more acceptable if SA3 is willing to define a more efficient mechanism in a subsequent release.

b) Comment: Two different mechanisms for UPIP mean that there will be two kinds of implementations on both UE and RAN, which will increase the complexity of the system

Response: As with any solution, adding a new mechanisms increases the complexity of the system, but we think the additional complexity is justified given that it will allow increased data rates with less overhead, e.g. leading to reduced battery consumption, etc. High data rates are an important selling point of 5G, so mechanisms that help to achieve this should certainly be considered.

c) Comment: It may increase the security risk since DU may not locate in a secure enough environment

Response: If you think the security of DU is not sufficient, we are certainly willing to help to work on solutions that will help mitigate the potential security risk. We can try to address this in the study or in possible follow-up work.

d) Comment: Currently PDCP layer IP is performed per DRB (which is corresponding with PDU session). DRB is invisible for MAC layer. It's not clear how to perform per DRB integrity protection if IP is done in MAC. Our purpose is to make integrity protection can be made up to full rate, but it does not mean integrity protection are mandatory used for all kinds of UP data. That is totally different. Also, the solution may bring some impact on the multiplexing function for MAC layer, which need to be evaluated by RAN2.

Response: Solution#4 works at the level of transport blocks, and basically means that all MAC traffic will be integrity protected. Given the limited overhead of the solution it can easily do this at full data rates, so no need to distinguish which traffic will be integrity protected and which not. Hence, we don’t think the multiplexing function for the MAC layer would be impacted. Note that also MAC Control Elements and PDCP Control PDUs will be integrity protected as well, which may lead to additional security.

**[email] China Mobile (Vice Chair):** Whether to provide integrity protection or not to specific should be based on operator’s policy. Not all user data need to be protected from operator perspective, like voice, streaming, etc. That is requirement the solution need to fulfill.

**[email] Philips:** There is no explicit requirement in Section 5 of 33.501 or service requirement in 22.261 that requires integrity protection to be switched on/off per service type. The solution to do the PDCP UP IP per service type/DRB (in Section 6.6 of 33.501) seems mainly driven by the overhead caused by the PDCP based integrity protection. If the overhead would be very limited, why would you not want to enable integrity protection for all user plane data, given the additional security it will bring?

**[email] China Mobile (Vice Chair):** That argument is not very useful for making progress. A similar argument can be made like there is also no explicit requirement that integrity protection to be provided as a whole. And we will fall into endless debating. The situation is currently we have specified integrity protection is provided in granularity of each PDU session, and we have shown the request for it. The discussion should base on that.

**Current Status: under discussion**

**Blockers: China Mobile, Nokia, Spreadtrum**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200700 Conclusion to Key Issue #5 Samsung

**[email] Futurewei:** Contribution S3-200700 should be noted. I agree with the comments from today’s conference call that suggest any other solutions (special DNN, use of (D)TLS, etc.) on top of UPIP can enhance the protection of UP signaling messages, but not as a replacement for UPIP. Therefore, the conclusion to key issue #5 as proposed in the contribution should not be agreed.

**[email] Samsung:** The proposed solution uses the UPIP for the protection of UP signalling messages. S3-200700 propose to use the UPIP and does not depend on the application layer protection. Depending on the capability of the device, a dedicated PDU session with UPIP activated at the PDCP layer is created to protect the sensitive messages. If the UPIP is activated for the normal PDU session by the security policy, then dedicated PDU session is not required. Request you to reconsider the comment.

**[email] Huawei:** I remember we discussed a lot on the solution #1 in the past few meetings. I don’t think this solution can address UP integrity protection very well. The main reason is that not flexible enough. For example, at least the network shall know how to distinguish DNS service and non-DNS service which means SA2 shall be involved definitely. Moreover, this will increase the complexity from network side. In we do this way, that means maybe in future we shall be able to set up a lot of different and dedicated types of PDU Session.

**[email] Samsung:** According to TS 23.501, IP Packet Filter Set is used to distinguish the IP packets using the following, (for example, for DNS port number is used and for ICMP, Protocol ID is used).

The SA2 specification already specified the mechanism for differentiating the IP packets and each packet is inspected to apply QFI. No new mechanism is needed for packet filter.

It is the other way, going forward UEs and gNB will support UPIP at full/higher data rates and establishment of dedicated PDU sessions will reduce. No need for interim solutions like application layer security is needed.

If it is suggested to check with SA2, then let’s send an LS from SA3 to SA2 to request their opinion on this solution.

**[email] Huawei:** My concern is to the two points:

1) The solution may work for aLTEr attack, but it requires all of the DNS servers which support and need UP IP are located in the same DNN if there are multiple DNS servers. This is different from the current implementation.

2) The solution can’t work for IMP4GT attack, because the attack can always pretend to be a HTTP server who is a normal DNN which does not configure “integrity required”.

So I don’t think the solution can be conclude like this.

**[email] Samsung:** My response to your concerns are as follows:

1) If multiple DNS servers are used in the network, then aLTEr attack is not possible, as the attacker cannot identify the destination IP address preciously. In such scenarios, network may not configure a DNN to protect the DNS or configure multiple DNN appropriately.

2) Further to my understanding, if the DNS redirection attack is not successful, then connecting with malicious HTTP server will not happen.

**[email] Huawei:** In my understanding, your argument is not correct because: The logic is that the DNS queries are done in a PDU Session towards the same DNN as the main use, likely to be the same PDU Session. So “the attack cannot identify the destination IP address” is wrong.

Simply to say, deploying in one way for certain services does not prevent deploying in another way for other services in the same network.

**[email] Samsung:** My argument is, if the UE is configured with multiple DNS server IP addresses, then attacker cannot guess which DNS server IP address is used in the encrypted packet coming from different PDU sessions to successfully redirect the packet to a malicious DNS server. If a DNS server IP address is used for all applications, then the proposed dedicated PDU session, once established will route all DNS requests to the UPF, where the DNS server is reachable. Even if different applications belong to different PDU sessions, using the IP packet filtering you can distinguish the DNS packets (using destination IP address and port) and send it the proposed dedicated PDU session. Since a DNS server is used, established PDU session can reach this DNS server, even though it is requested by different applications.

**[email] NCSC:** I believe your argument below doesn’t hold if we consider a real-life attacker. You say the attacker needs to know the IP of the DNS server – but if they see a small handful of DNS requests then they can try aLTEr-ing them one by one against the set of know server IPs, until one works. In real life, any aLTEr attack won’t work 100% of the time anyway, so there’s already an element of probability of success that the attacker will accept – having to narrow done the target DNS server IP address from a choice of 10 to 1 is within their acceptable effort. Also DoT only protects against aLTEr if using a network DNS server (set up for DoT), it doesn't protect against a UE using another DNS server. So you would require ALL DNS servers that the UE could possibly ever connect to to be using DoT to mitigate. Or we can just use UPIP – it’s cleaner, and solves more problems.

**[email] Samsung:** Since the attacker is working on the encrypted packet, he should make the best choice in guessing the Dst IP address in the first attempt itself. If first attempt is wrong, the he cannot use the same PDCP Count to make second attempt. Also if there are many DNS server, then the requests does not have any dependency. I agree, UPIP to be used and S3-200700 uses UPIP.

**[email] NCSC:** I’m sorry, I must have explained myself badly. I didn’t mean that the attacker would try several attempts on one packet, but rather that they would repeat the attack on each encrypted DNS request that they detect, trying a different destination IP for each one (or re-trying the same destination IP if the UE is likely to jump between different servers). Given the number of DNS requests a UE will send out, then at some point the attacker will succeed, which is enough for them to redirect one DNS request and get a way in. But maybe we’re having an unnecessary agreement, as we both support UPIP over a solution at the application layer.

**Current Status: under discussion**

**Blockers: Futurewei**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200768 Proposed conclusion for Key Issue #6 in TR 33.853 Qualcomm Incorporated

**[email] Ericsson:** We agree to use 5G UE Security Capability IE (see 9.11.3.54 of TS 24.501 [10]) to indicate that the UE supports user plane integrity protection with an ng-eNB. But we are not sure about to use one of the bits that are allocated  to indicate support of an EEA or EIA algorithm in UE security capability IE.

When we did EN-DC – option 3, SA3 concluded to not use any of the bits that are already allocated to indicate support of an EEA or EIA algorithm in UE Network Capability IE in Attach/TAU request, to indicate support for NIA and NEA algorithms. But you  don’t see this as a problem in case new algorithms are supported in EPS/LTE in the future?

**[email] Qualcomm:** Thanks for your comments. Glad to know that you are ok to use 5G UE Security Capability IE. The reason we prefer the use of one of the allocated (but unused) algorithm bit instead of spare bits is that use of allocated bits will not impact any of the legacy nodes in the path (AMF or RAN nodes), whereas latter would impact not only the AMF (as it has to do the mapping before sending it to the ng-eNB) but also when these mapped info is passed through legacy RAN nodes (i.e., nodes that do not understand these new mapped bits), the mapped bits will be lost. We do agree that when we do run out of unused (but allocated) bits then extending them (e.g., to accommodate more algorithms) would impact NAS/AMF. Since here we only need one bit, we would still be left with two unused bits for future use.

**[email] Ericsson:** Thanks for clarifying. I am fine with your reply.

**Current Status: under discussion**

**Blockers: None**

**Expected Status at end of meeting (unless there are further comments): Approved**

# S3-200632 draft WID - Normative changes for UPIP VODAFONE Group Plc

**[email] Telecom Italia:** Telecom Italia would like to support this contribution.

**[email] Qualcomm:** For the record, I propose this contribution be noted.

**[email] DT:** Deutsche Telekom is going to support this WID (assuming that it’s Rel.-16).

**Current Status: No Comments**

**Blockers: Qualcomm**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200633 CR to 33.501 - Update to User Plane Integrity Protection VODAFONE Group Plc

**[Email] Telecom Italia:** Supports this document

**[Email] Samsung (Vice Chair):**

1) NOTE 2 is not clear in the contribution. Particularly on “disable it only by exception”, needs clarification. What are these exceptions? Which working group in 3GPP decides these exceptions? Need a detailed study on these exceptions in 3GPP.

2) If the UP-IP is disabled for a PDU session or for a UE (for what so ever reason), then how the GSMA referenced attack is mitigated?

3) Need further study and analysis on activation of the UP IP at full data rate (for the supported data rate). As there are, many issues to be addressed by the SA3 in collaboration with other working groups, for example, ambiguity in handling of UP integrity check failures, c.f., TS 33.401, clause 7.3.2 (NOTE). Not all such issues can be identified and addressed in Rel-16 timeframe.

4) Instead, S3-200696 by Samsung should be considered to mitigate the GSMA referenced attack for Rel-15 and Rel-16.

Proposal: Further study in collaboration with other working groups is definitely needed for activation of UP-IP for all supported data rates. Therefore, this CR should not pursued.

**[email] Futurewei:** I support the Vodafone contribution. One minor change suggestion in the proposed NOTE: please remove “for all data rates”. It is clear the recommendation is for all data rates.

I don’t agree with Samsung comments and proposal. Addressing the issue raised from GSMA is orthogonal to having full data rate UPIP in 5G. The 3GPP community designed 5G to support UPIP at full data rate. It is a fundamental right in 5G, not a privilege.

**[email] Qualcomm:** Qualcomm does not agree with this CR. We propose that it be not pursued.

- We also share some of the concerns expressed by Samsung in this thread.

- Furthermore, as described in S3-200766, mandating support (as this CR proposes) without also mandating its use does not really address the identified threats

- Per existing R15/16 specs, UE can already support UP IP at full data rate - therefore this requirement can be enforced in operator networks where it is really needed.

- It is unclear what is meant by “for all supported data rates”

- 5GS is designed to be flexible in order to support different use cases/services/device capabilities – this is why keeping the existing UE based capability negotiation is important to keep this flexibility

- As proposed in S3-200767, we would like to consider mitigations that actually address the identified threats not only in 5GS but also in EPS

**[email] CableLabs:** I support this CR from Vodafone. Although I also appreciate the proposals from Qualcomm and other companies on mitigating some related attacks such as DNS hijacking using specific solutions (e.g., DNS over TLS), UP IP at full data rate provides a fundamental security property (i.e., data integrity) that will mitigate not only known attacks (such as DNS hijacking, IMP4GT) but also unknown attacks that exploit the lack of data integrity (as indicated by Steve Babbage’s email on another thread). Regarding the comment from Samsung on “disable by exception”, I think the exception can be made based on operator policy. I would expect that the decision to disable UP IP will be made consciously by an operator who would understand and accept the risk and may implement other protection to mitigate some of the risk.

**[email] Huawei:** In general, I support this CR. But I also think “for all data rate” could be removed in the NOTE since it’s very clear that we don’t want any limitation on data rate point. What we need to do with first priority is informing to other groups on this proposal, e.g. RAN2, CT1, SA2.. Moreover, I agree that the deactivating UP IP shall be executed because of those exceptions based on operator’s policy. This is reasonable.

**[email] OPPO:** OPPO proposes that the CR is not pursued for the time being, due to some reasons below

1) We think "mitigation to GSMA referenced attack" (which has been somewhat proposed by QC and Samsung) is a more reasonable way.

2) Further study in collaboration with other working groups is needed for activation of UP-IP for all supported data rate

**[email] Samsung:** @Marcus: If “The 3GPP community designed 5G to support UPIP at full data rate. It is a fundamental right in 5G, not a privilege. “ then why S3-200643 proposal #3 gives option for UPIP deactivation. It should be mandatory to activate for all UP traffic, as done for control plane messages?

@Tao: Why operator (serving / home) need a policy to give exception, when the system support the capability?

Also if “I would expect that the decision to disable UP IP will be made consciously by an operator who would understand and accept the risk and may implement other protection to mitigate some of the risk.”, then why it is mandatory requirement for the UE and the gNB to support UPIP for all supported data rates?

Would like to emphasis again, Need further study and analysis on activation of the UP IP at full data rate (for the supported data rate). As there are, many issues to be addressed by the SA3 in collaboration with other working groups, for example, ambiguity in handling of UP integrity check failures, c.f., TS 33.401, clause 7.3.2 (NOTE).

**[email] Vodafone:** Oppo wrote: We think "mitigation to GSMA referenced attack" (which has been somewhat proposed by QC and Samsung) is a more reasonable way.

For the reasons I gave in my email on Monday, Vodafone thinks it would be very short-sighted just to mitigate one particular exploit that has been discovered already, rather than to prevent further exploits of the lack of UPIP.

Qualcomm wrote: Per existing R15/16 specs, UE can already support UP IP at full data rate - therefore this requirement can be enforced in operator networks where it is really needed.

Vodafone feels it is quite clear that some UEs cannot support UPIP at full rate. That is exactly the issue that we are trying to solve.

**[email] Telecom Italia:** would like to support Vodafone view. Mitigation measures proposed by Qualcomm and Samsung could also be useful for the specific scenarios they were proposed to address, but SA3 should not give up looking for a solid solution like having UP IP supported up to the full rate. When available, SA3 should aim to specify solid solutions, rather than being fine to specify urgent and specific workarounds potentially triggered by new attacks (including possible variants of already known attacks, that were addressed only with a specific “mitigation” that suddenly becomes not sufficient).

**[email] Telecom Italia:** Referring to Qualcomm's comment "Furthermore, as described in S3-200766, mandating support (as this CR proposes) without also mandating its use does not really address the identified threats"

Telecom Italia would like to say that 3GPP standard is plenty of features that are MANDATORY TO SUPPORT and OPTIONAL FOR USE. And this pure fact is definitely not new... 😊 😊 Ciphering is perhaps the most evident, the most famous example since ever. Just “being a feature optional for use”, e.g. based on a MNO policy, does not mean that such a feature does not worth “to be mandatory to be supported” as your comment seems to hint.

Having UP IP supported up to the full rate would allow the MNOs to decide if and when to activate it, or not activate it, for whatever service, and then the MNO would have the tools to address the identified threats, and also others that might arise in the future... (if the MNO wants, or will want, to do it).

**[email] China Mobile (Vice Chair):** China Mobile would like to support this contribution in general but with small modification on newly added Note2 as following:

"NOTE2: It is strongly recommended to activate user plane integrity protection by default for all data rates and deactivate it with operator’s policy."

We don’t believe not to use up ip is just exception. Whether to use or not shall be well defined by operator’s policy. And we fully support the argument made by Mauro in following email.

**[email] Ericsson:** Ericsson has a similar comment to this contribution as to S3-200737/S3-200738: In clause 5.3.3, its very unclear what "all supported data rates" means or implies to the gNB, and we don’t support the proposed update to the gNB in clause 5.3.3 in TS 33.501.

**[email] Huawei:** I’m confused a little. In my view, the gNB already supports the UP IP since the full data rate definition already exists there, what we need to do is to specify the value of it. So what’s the problem of gNB side? Can you explain?

**Current Status: Under discussion**

**Blockers: Qualcomm, Samsung, OPPO**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200696 UP integrity protection for UP Signalling messages Samsung

**[email] Huawei:** My understanding is this CR shall not be pursued. It’s relying on the S3-200700 and S3-200695, and 200695 was already agreed to be noted. The main point is still that we don’t think establishing the new dedicated PDU Session can resolve the UP integrity protection issue sufficiently. Moreover, if we include this kind of procedure, we at least involve SA2 to consider because of session establishment procedure definition. This increases complexity currently.

**[email] Samsung:** There is no dependency on the disc paper S3-200695 and the CR S3-200696. S3-200695 just introduced the CR. Can you please provide little more details on, “we don’t think establishing the new dedicated PDU Session can resolve the UP integrity protection issue sufficiently”. There is no modification to the PDU establishment procedure, as the proposed solution is already in line with the SA2 and CT1 defined procedure.

**Current Status: Under Discussion**

**Blockers: Huawei**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200697 Integrity protection of DNS messages Samsung

**[email] Huawei:** The CR shall not be pursued. It implies some changes affecting the existing network a lot. For this sentence, “EPC should be able to support the configuration of necessary credentials in the UE for the protection of the DNS messages at the application layer”, how does the EPC support to configure this kind of credential? Besides, it’s a little bit strange only the DNS security emphasized in the whole security specification for LTE.

**[email] Samsung:** Mechanism to configure this kind of credentials can be done along with the DNS IP address and it is up to the Stage 3 working group(s) (CT1) to specify. Discussion on the contribution S3- 200767 in yesterday’s conference call, which suggest the same solution, the chair notes mentions that “no objections to m1”. If application layer protection is not used, then how to mitigate the GSMA referenced attack on DNS for EPC (which does not support UP IP).

**[Conf Call] Samsung** presented doc.

**[Conf Call] Vodafone:** is this CR for LTE?

**[Conf call] Samsung:** yes

**[Conf call] Vodafone:** it does not seem efficient we should protect all communication as per my earlier comments. We don’t object to this CR but prefer a wider solution.

**[Conf Call] NCSC:** We agree with Vodafone

**[Conf call] DoCoMo:** is the added text a note?

**[Conf Call] Samsung:** yes it is a note.

**[email] Huawei:** The NOTE is still unclear to me and also will cause confusion to other groups. We need to know the following points very well.

1) What’s the meaning of “necessary credential”? Who or which group determines it?

2) How does EPC support for those credential? Current situation is only USIM based credential is used by EPC.

3) What’s the meaning of application layer protection here? DTLS? DNS-TLS or HTTPS?

I’m not objecting we should use measures to defend the attack raised by GSMA on DNS redirection or modifying the DNS request which 200767 meant to I understand.

However, there are two things, this proposal S3-200697 is a specific CR proposing the change to 33.401 LTE, and those changes are not clear enough.

**Current Status: Under Discussion**

**Blockers: Huawei**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200618 Mandatory User Plane Integrity for 5G GSMA

**[email] Chair:** proposes to postpone as there are no direct replies

**[email] Rappourteur (VF):** proposes to note as actions are being taken as a result of the LS and the response would come from SA or RAN not SA3.

**[Conf Call] Vodafone (Rappourteur):** Propose to note this document as there are now inputs based on this document and SA3 would not be the one to reply to it as other groups are involved too.

**[Conf Call] Chair:** This document in Noted (now).

**Current Status: Final Status - Noted**

# S3-200643 UPIP Way Forward Discussion Futurewei

**[email] Nokia:** S3-200643 cannot be endorsed.

It proposes,

1 Mandate all UEs to support user plane protection without data rate limitations.

2 Mandate all gNBs to support user plane protection without data rate limitations.

3 The use and activation of user plane protection in 5G is to be an operator choice, based on user plane security policy.”

Proposal 3, I can agree with. Proposal 1 and 2 are very open ended, they are not practical or necessary.

**[email] Futurewei:** Actually, Proposals 1 and 2 are very specific. UPIP is one of the big improvements over previous generation of 3GPP networks. This is what 5G is designed to do. In my view, 3GPP and SA3 made a mistake by allowing certain UEs with UPIP rate limitation to exist in R15 and we should not make that mistake again. UEs may have other different capabilities, but having different security capabilities essentially allows different “class” (for lack of a better word) of UEs to exist in the same 5G network is not acceptable. All UEs in the same release should have the same security capability.

**[email] Qualcomm:** We also share the same view as Nokia - S3-200643 cannot be endorsed. The motivation is explained in our contribution S3-200766.

**[email] Spreadtrum:** Spreadtrum would second Nokia and QC: S3-200643 cannot be endorsed

**[email] OPPO:** We also share the similar view in QC's paper (S3-200766). We think we just focus on the issues raised by document (aLTEr and IMP4GT attack) and trying to resolve them, rather than mandating the "full rate of UPIP". So the S3-200643 cannot be endorsed.

**[Conf Call] Nokia:** It is already covered in TS 33.501 and in our view the need is not important enough to mandate for all data rates.

**[Conf Call] Not presented** due to audio issues with Marcus.

**[Conf call] Telecom Italia:** We see this as important to support.

**[Conf Call] Vodafone:** We don’t understand what Nokia means by the current spec is sufficient - Vodafone see that the current situation ends u in handset not supporting UPIP - Vodafone Support.

**[Conf Call] Huawei:** We support this

**[Conf Call] Orange:** We support this - have a slight word change - "at full data rate"

**[Conf Call] Samsung:** Not in favor of this - if we give an option to enable and disable this why does the UE / gNB need to support it maditory.

**[Conf Call] DT:** We support this paper

**[Conf call] Qualcomm:** This paper is on LTE not 5G so is a different question to the one for 5G. We do not believe full rate UPIP is sufficient unless it is mandatory to use too.

**[Conf call] Erricson:** Answer gNB support. - there is no requirement for the gNB for UPIP so it seam odd for the mandatory support in the gNB to be extended to the gNB.

**[email] Vodafone:** Qualcomm, On today’s conference call, you stated your belief that:

• some R16 UEs should and will support UPIP at full data rate;

• but this shouldn’t be mandated for all R16 UEs. I think you had in mind low cost or limited use UEs – am I right?

I’d like to dig a bit deeper into this. As a completely hypothetical example, I can imagine that a low cost device might:

• be able to support user plane traffic, with encryption, at 1mbps;

• but if UPIP is activated, only be able to manage 800kbps.

In such a case, for such a device, is that extra speed really important? Can’t we just say that this device supports 800kbps? Can you give a plausible example of a case of a device type where the speed difference between what it can manage with UPIP, and what it can manage without UPIP, would really matter to the commercial viability of the device?

**[email] Qualcomm:** My point on the conf call was that R15/R16 specs already allow support of UP IP at full data rate and therefore, can be implemented at the choice of the UE vendors depending on the market need and use cases. We do not see an need to mandate it via specs. As also noted few times already, just mandating support alone is not sufficient unless use of it is also mandated (similar to what we do for NAS control plane for example).

**[email] China Mobile (Vice Chair):** I found the discussion on this contribution has split into two email threads. I hope the discussion can be merged as only one thread. We support all the proposal in this contribution and hope it can be endorsed. For Anand point that mandatory to use, I think Mauro’s comment in another email thread (S3-200633) has a clearly reply.

**[email] Vodafone:** From a pure security point of view, making sure that all UEs support UPIP at all rates is clearly the safest thing to do. You, I think, are saying that there’s value in allowing some UEs not to do this; I’m trying to understand where that value is. At the moment, I can’t see it. Can you (or anyone else on this thread) give examples of device types where there is commercial value in not supporting UPIP at every rate offered by the device? This could, for example, be:

• devices where the production cost of supporting UPIP makes them commercially unviable;

• devices where extra speed can be achieved without UPIP, and where this extra speed has commercial value.

Unless there’s some perceived value in allowing devices not to support UPIP, I can’t see any reason to reduce security by doing so.

**[email] Huawei:** I support your view.

I think your example is very helpful. I’m trying to make the following standard translation:

There is an indicator in PDU session establishment Request message, named integrity protection maximum data rate, which indicates to the network the maximum data rate per UE for user-plane integrity protection for uplink. It’s UE security capability related.

Currently, there are two values, i.e. 64kbps, and full data rate. That means, if the UE indicates 64kbps to the network, the network will know, “if I activate UP IP for this UE, the UE could only support data rate transition under 64kbps, so, I couldn’t activate UP IP for it (This is defined in 5.10.3 in 23.501).” if the UE indicates full data rate to the network, the network will know, “if I activate UP IP for this UE, the UE could only support full data rate, so, I could activate UP IP for it since the UE has good performance (This is defined in 5.10.3 in 23.501).”

However, the reality is, 64kbps is too low for a UE, full data rate is too high to a UE. In order not to be turned off by the network, the UE can only indicates 64kbps to the network, then, the UP IP is actually deactivated. Thus, we proposes to extend this value, to identify more specific values (full data rate does not have specific value), e.g. 1Gbps, 2Gbps, etc. Thus, the network could judge whether to activate UP IP for a UE, and the UE shall report this value.

**[email] Vodafone:** As I said in my previous mail, the best thing from a pure security point of view is simply to make sure that all UEs support UPIP at all rates. If that’s done, then your proposal to introduce a finer grained way for the UE to state “this is the highest rate I can support with UPIP” is not needed. I haven’t yet seen a convincing reason not to have all UEs supporting UPIP at all rates. That’s the point of my question to Anand. If it turns out that there are sufficiently good reasons to allow UEs that don’t support UPIP at all rates, then I will support your proposal. Of course, it needn’t just be down to Anand to answer my earlier question: anyone is welcome to give a use case where it’s better NOT to support UPIP at full rate.

**[email] Telecom Italia:** since SA3 is supposed to be a Security WG, I would like to see SA3 providing guidance driven by security, that is to make sure that all UEs support UPIP at all rates as Vodafone suggested.

**[email] OPPO:** In my opinion, some of the problems may incur if the full rate UPIP is the only choice: The (Integrity Protection) IP can be much more resource consumption than encryption. (for CP, the UE uses the NEA to calculate a streamblock once and just use the streamblock to "xor" each PDCP SDU, however for IP, for each the PDCP SDU, it needs to use NEA to calculate a MAC and do the comparison).

Thus two critical problems may incur from our UE vendor perspective:

1) The E2E latency may not be guaranteed, the UE may not calculate all the data in time. The network have no idea about the capability of UE for IP and if too much data are being transmited, then the UE will fail to gaurantee the QoS.

2) The power consumption will be much higher. This may be serious especially when User select "power saving mode".

We do not want to see some unnecessary IP occurs. Actually, the issues referenced in GSMA only touch the DNS request and ICMP message explicitly, and if we can deal with this two isseus, it seems no problem.

**[email] Vodafone (Rapporteur):** You say that the power consumption would be much higher…. Do you have any published figures or research papers for the increase in power consumption that we can use as facts in the TR?

**[email] DT:** In my opinion we (as SA3) should worry about the security requirements much more than a potential “the UE may not calculate all the data in time”. I haven’t seen convincing arguments for this so far from any vendor. Comparable systems such as 802.11 already include UPIP as standard at all data rates. Further, our understanding is that the processing required for cryptographic computation is only a small proportion of the overall processing load involved in traffic transmission and reception across all layers. Although GSMA referenced (this time) only to that particular attacks – it doesn’t mean that we should limit our scope only to react. Why not conclude and avoid any tampering of UP data for the future? Deutsche Telekom beliefs that to make sure that all UEs support UPIP at all data rates from Rel.16 onwards should be the way forward.

**[email] Samsung:** Would like to know, Why SA3 need to provide an option for disabling the UPIP? For encryption it is understood that, there are regional regulatory requirements and limitations (from LI groups), so SA3 recommends and does not mandates its usage. For integrity protection, there is no such limitations from security point of view. Further, based on SA plenary task “SA tasks SA3 to determine how to mitigate identified security problems associated with user plane integrity from Release 16 onwards……….”, we need to identify the solution, but if we disable UPIP, we are not solving the problem. We are discussing, the UE and the gNB should support UPIP at full supported rate, but network has option to deactivate the UPIP. If SA3 specifies UPIP can be deactivated then, SA3 need to specify how the identified threats are mitigated. From my understanding based on the e-meeting discussions, there are two options:

1) Accept the limitations in supporting/enabling UPIP at full rate and also current 64 kbps UPIP capability is too limited. If SA3 decided to have more granularities for UPIP capabilities, then SA3 should request RAN2/CT1 work on defining more granularity for UPIP data rates. Identify solutions on how best the threats (on DNS and ICMP) can be mitigated with the new more granularity for UPIP data rates.

2) Make sure that all UEs support and activate UPIP at all rates.

Option 2) needs more study on the issues like failure handling/reporting/performance and there is no time to do it in Rel-16 (Complete analysis given in S3-200695). GSMA referenced attack is not new to SA3, SA3 discussed similar attack for Relay Node (manipulation of Dst IP address) and TS 33.401 supports UPIP between RN and Donor eNB. Please note that, SA3 identified serval issues when specifying UPIP and mentioned a note like, implementation can honour the packets even integrity check fails, as to maintain the system performance.

**[email] Telecom Italia:** Same view as Thomas (DT).

**[email] Telecom Italia:** (To Samsung) 3GPP supports the possibility for a MNO to use - or not use - the encryption since ever and this possibility has never been a valid argument to say that then “there is no reason to support encryption”. Sorry, your argument does not hold. Being Mandatory to support and Optional for use is something totally possible in 3GPP specs. I think that the MNO need to be put in a position to decide if a certain service require - or not require - UP IP (and if UP IP is deemed as needed, then it shall work without any rate restriction).

**[email] Samsung:** OK. If the MNO disable UPIP, then GSMA referenced attack is possible, SA3 need to address this scenario also using an alternative mechanism? Further, based on your comments, TS 33.501 is all set from Rel—15 to mitigate the referenced attacks. TS 33.501 does not have rate limitation. Other specs utilising the option of enabling or disabling UPIP by considering device capability as one of the criteria and other criteria like requested application, like so. If we remove only the device capability criteria, still considering the application capability other specs utilising the option of disabling UPIP and can disable it. SA3 need to address for this scenario also? . For example, suppose SA4 may tell for voice over 5G application, UPIP should not enabled for codec performance. In this case, even UE supports full rate UPIP, for voice over 5G MNO cannot enable it and attack on this PDU session is possible. For such scenarios, the proposal in this contribution does not hold good.

**[email] Vodafone (Rapporteur):** I can see 3 possible scenarios where the network operator may disable UPIP.

1. At the request of the customer where the customer is for instance an enterprise customer running a proprietary protocol that already has UPIP protection (I see this as an exception case)

2. Where an enterprise customer has roamed into an area that does not have any network operators that support UPIP full rate (as they have R15 networks) and where the customer would be denied service from any network if UPIP is mandated in that location. In this circumstance, the rate is either limited to the available rate that is UPIP supported or if the customer accepts the risk (maybe because they are using VPN), full rate without UPIP may be allowed. (This scenario is problematic and may not be realistic).

3. Because the service being used does not transmit any signalling over the UP (but in this case having UPIP on is probably best).

I cannot directly see any consumer cases for not using UPIP. I am struggling to find any other cases….

**[email] Futurewei:** I totally agree with Tim, Mauro, Thomas, Steve, Minpeng and the rest of operators who voiced support for this. UEs may have different capabilities, but security capability should be all the same. This argument that we don’t want to mandate full rate UPIP because some UEs or UE vendors may not support the security capability SA3 already defined is not a valid argument. Additionally, that was the same argument two years ago. If we continue to let this happen, 3GPP is not only weakening the security of 5G but is also allowing the UE market to be fragmented. Using or not using UPIP should be based on operator’s network policy, not because some vendors choose not to support UPIP or don’t want to support UPIP at full date rate on their UEs.

**[email] NIST:** We agree with everyone who has voiced support for this and would like to see full rate UPIP available in all UEs. Fragmenting the UE market will create two classes of UEs from a security perspective, a more secure class and less secure class. This will also highlight/create a problem that there is very little transparency to organizations and subscribers about their UE's security capabilities. Will organizations need to specify in procurement language that only the 'more secure class' of UEs will be acceptable to meet an organizations security requirements?

**[email] Broadcom:** First a disclaimer that this discussion is implementation dependent. I believe that no one disagrees with the fact that there is a computation cost to be paid for applying the integrity protection. The cost is given by the CPU clock cycles, memory Read/write operations and bus transfers. If you do compare encryption vs integrity protection operation there is no way you can come with a lower cost of the encryption comparing with the integrity protection mainly due to the memory write operation for the whole PDU typically an order of magnitude or more than the CPU utilization. This is why I would be very curious to know the data based on which you make such claims.

**[email] BT:** Fully support all the arguments made in support of full rate UPIP available in all UEs. In addition we have now discussed this in an open forum and provided evidence we knew that we could address the published vulnerabilities and related vulnerabilities that may be published in the future. [or nobody has provided evidence that there is actually performance issue, in fact, a statement was made yesterday that all devices can be enabled with UPIP at full rate ] Therefore would it be reasonable to say we can’t then use the “start of the art” defence in any possible action from those customers who have the “less secure class of device” On the option for operators to disable UPIP, the only case would in POC’s and trials for new services, otherwise, except in the case of, as Tim says of a documented request of the customer, it would always remain enabled.

[email] Samsung: (To Vodafone) Security concern with the scenarios you mentioned for example:

1. At the request of the customer where the customer is for instance an enterprise customer running a proprietary protocol that already has UPIP protection (I see this as an exception case)

Before establishment of the UPIP at application layer or even before sending the initial request to the server, the UE will resolve the IP address of the enterprise server using DNS without UPIP.

**[email] Qualcomm:** I agree with the responses from Oppo and would add some additional response below wrt the questions that you addressed to me in this thread.

• It may be use case dependent (e.g., achieving latency/power consumption/peak data rate is more important than OTA UP IP; and security is achieved by means other than OTA UP IP, e.g., AS layer security is not sufficient and e2e security is needed for the use case. BTW, I am sure you will agree that most services today employ such security rather than relying on just AS security for user plane.

• Yes, there is also resource impact (due to the need for provisioning additional hardware to achieve peak data rates) and we cannot assume this is acceptable for all UE device categories and tiers

Furthermore, as noted few times already, just mandating support of UP IP does not even address the threats identified in GSMA LS unless the use of it is also enforced.

Therefore, we continue to maintain our position against proposals mandating support of full rate UP IP for all UEs. I hope we can move past mandating support for full data rate and consider other ways of mitigating the threats identified in the GSMA LS.

**[email] Vodafone (Rapporteur):** (To Samsung) Not always, they may use fixed ip addresses or be a non-ip channel.... I do agree that the senario is an exception but I was trying to find common ground with you...

**[email] Spreadtrum:** Spreadtrum shares the view from QC and OPPO below, and holds the position against proposals mandating support of full rate UPIP for all UEs in R16.

**[email] OPPO:** I am not a productline guy☺, and just provide the technical analysis which explains why currently the UE may not support full datarate (in other words, needs to report a capability). I guess some similar discussion might happen in LTE era, where it not regulat the UPIP as mandatory also.

For FIorin's comments, I may go a little deeper form my understanding:

For CP, it is easy to use the "streamline" architecture, where all PDCP SDUs are just inputed to "xor" function and get the output. The delay would be the certain value (i.e. the time used for "xor" functionality) regardless of how much data inputs;

However, for IP, when the required number of blocks for IP functionality will be increasing as the number of PDCU SDU increases and there is no upper limits. As the resource is almost defined when Place and Route is done in IC design, it is not easy to simply shift some resouce for other functionality to IP functionality as requested.

**[email] Vodafone:** Anand (Qualcomm),I appreciate your reply, but I have to stay that this still seems very hypothetical to me, compared to the simple requirement for reliable security. You seem to be asking for the freedom to be insecure, just in case …. If you went to IETF asking them to allow some TLS clients not to support integrity protection, they would laugh at you.

**[email] Telecom Italia:** Same view as Steve (Vodafone). To me it looks really unbelievable that some Vendors insist to object in SA3, that was supposed to be a security group, against a security feature that is clearly asked by all the Operators and that is part of TS 33.501 since the beginning. I think that SA3 should still remain a security group and dictate the security guidelines to other WGs.

**[email] Qualcomm:** This view or analogy of either of you does not seem sensible to me. The sensible comparison to TLS/IETF would be for you to propose to always mandate the use of integrity protection just like in TLS (and as we do for NAS control plane for example).

Obviously, 3GPP decided to not to do as for TLS for 5GS. And neither of you are now proposing that we do that!

**Current Status: Under discussion**

**Blockers: Nokia, Qualcomm, Spreadtrum, OPPO**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200695 Proposed solution for UP IP issues in GSMA LS Samsung, Nokia, Nokia Shanghai Bell

**[conf call]** Presented by Samsung - can be noted

**[Conf Call] VF (rapporteur):** We feel that the LS underplays the risks and will add comments by email for the minutes.

**[Conf call] Chair:** Propose to Note

**[email] Vodafone:** "Vodafone have no objection to introducing additional security measures as a further line of defence, but I think it would be a mistake to see these as alternatives to full rate user plane integrity protection.

• The aLTEr attack, published in mid-2018, targets DNS; the LS S3-200618 from GSMA refers to as yet unpublished attacks that target other protocols. Ad hoc defences protecting against these attacks, if standardised now, will at best come into effect in 2021.

• It is highly likely that further exploits will be found, attacking other application layer protocols. Maybe they will be discovered first by responsible researchers ... or maybe they will be discovered and exploited in secret. If we only introduce ad hod defences protecting these protocols - if indeed it is possible to do so at all - after the attacks become known to us, then there will again be a period of years between first risk of exploit and availability of defence.

• Some of the contributions downplay the significance of the attacks already identified. But attacks only ever get better.

It is far more robust and responsible to protect against this whole class of attacks by implementing and activating user plane integrity protection, than to try to counter new or improved individual attacks (belatedly) after they are discovered.”

**[email] DT:** supports VF's minuted comments

**[email] Futurewei:** Additional security mechanisms and good security practices on top of UPIP can only add to the security to protect against attacks raised by GSMA, but they are not replacement for UPIP

**[email] Samsung:** agrees that UPIP should be used in 5GS and not to depend on application layer protection or additional security mechanisms. S3-200696 by Samsung uses UPIP (without any modification and just by configuration) to address the identified attacks (not only DNS but also other sensitive protocol messages like ICMP).

**[email] Vodafone:** S3-200696 makes sense to me if/when the following conditions are true:

(a) Application layer signalling can be identified and directed onto a dedicated DNN.

(b) The impact of integrity protection on the entire user plane is too great, so we prefer to apply it only to this dedicated DNN.

(a) may be true in some cases, but it would be unwise to suppose that it’s always true.

**[email] Samsung:** As I mentioned in the [S3-200700] e-mail thread, for (a) we can get opinion from SA2/CT1 on its feasibility.

**[email] DoCoMo:** this assumes that we only care about application layer signalling that the visited network knows about. If any new application comes around, then it will could end up being unprotected.

**[email] Samsung:** If an application is not DNN aware, the URSP will help with that. URSP rules will indicate which DNN/S-NSSAI to use for a type of traffic. For example, URSP rules could contain an IP filter where destination port is 53 for DNS. Details of UE Route Selection Policy (URSP) is specified in TS 23.503, Clause 6.6.2. URSP is always up-to-date in the UE.

**[Final Status]** As the decision to Note this document was not challenged by the 1st deadline it is now has the final status of NOTED.

**Current Status: Final Status - Noted**

# S3-200737 Discussion on endorsement for UP IP Huawei, Hisilicon

**[Conf call] Presented by** Huawei

**[conf call] Nokia:** you are referring in the doc about work if they are already working on it why do we need to send them an LS.

**[Conf call] Huawei:** because they need further security information

**[Conf Call] Vodafone:** we support this

**[Conf Call] Qualcomm:** We have already discussed that we do not support UPIP at maximum data rate. It is not clear enough to endorse.

**[Conf Call] Nokia:** I am also not clear on the advice being requested.

**[Conf call] Samsung:** We are not in favour of this contribution because it does not say how the attacks are mitigated.

**[Conf Call] Huawei:** Here we are saying that full rate support is required.

**[Conf Call] Qualcomm:** believe that UEs can do full data rate - so no need to change.

**[Conf Call] Telecom Italia:** but we need to be able to rely on the support to turn it on.

**[Conf Call] Apple:** Can all UE support full data rate.

**[Conf Call] DoCoMo:** not mandating it creates a mess when trying to setup this service in by the network operator. It is different for special service UE's as they can be managed by a special process

**[email] Huawei:** Thanks for the meaningful discussion about the document S3-200737 and we revise it according to all the opinions by revision r1. All of you can check the revision in the draft folder.

My intention is that since SA plenary gave us the following guidance, and bunch of WGs are involved as well as RAN plenary. We shall consider and give our suggestions to other groups to identify the impacts and potential changes to R16 specs, because UP IP is created by SA3 in 5G phase.

“SA tasks SA3 to determine how to mitigate identified security problems associated with user plane integrity from Release 16 onwards for UEs supporting Standalone NR connected to 5GC, including the proposal to mandate the support of full rate user plane integrity protection for those UEs, and report their progress at the next plenary. The SA3 meeting schedule is left for discussion in the SA3 working group. SA3 should make necessary arrangements including coordination with other groups to complete the work in R16.”

Therefore, in this document, we try our best to identify those need to be revisited clauses related to UP IP procedure. E.g. SA2 may need to modify the PDU session establishment procedure because of User Plane Security Enforcement;

CT1 and RAN2 may need to define or check the data rate which is closely related to UP IP usage. Some companies comment that those are not security requirement, I don’t think so. That’s the root cause why the UP IP can’t be supported, so it’s very necessary to tell the other groups how to adopt UP IP with data rate definition clearly. However, in order to make the whole thing proceed and align with SA request, I made the changes in this revision, please check:

Proposal 1: In R16, other maximum data rate value(s) which don't restrict the usage of UP IP need to be defined. SA3 is kindly requested to send LS to SA2, RAN2, RAN3 and CT1 to inform the guidance.

I hope this proposal is acceptable.

**[email] Telecom Italia:** Telecom Italia does not support this contribution, not even in the revised version. SA3 never put restrictions on the supported data rates and SA3 is supposed to put security requirements that need to be met by other WGs. The restriction to apply UP IP only up to 64kbps was added elsewhere before the ALTEr attacks were spotted and now the situation is different. SA3 guidance should reflect the current status, based on security requirements and not based on “what we could probably find on the shelf”. 3GPP should drive what need to be put on the shelf to have a secure 5G system, and it should not work on the other way around... The restriction on UP IP added elsewhere needs now to be removed from Rel-16 onwards FOR SECURITY REASONS and this is what SA3 should ask and clearly promote. SA3 should not legitimate/encourage a proliferation of MEs with different capabilities: this would fragment the market and would put the MNOs in serious troubles since the MNO cannot prevent a User to buy the ME they want. I am also reluctant to see SA3 providing concrete suggestions on how to change TSs that are out of the scope of SA3. I would be happy to see SA3 willing to work on the security-related specs and let other WGs to behave accordingly. They are certainly able to do it. I would also object to start a new ping pong with other WGs: SA3 should put the requirements and other WGs should go along with them.

**[email] DT:** Deutsche Telekom is sharing Telekom Italia’s view and does not support the proposal made in S3-200737.

**[email] Broadcomm:** Broadcom has a similar position as the one stated below by TI and DT

**[email] Ericsson:** Ericsson has a similar comment to S3-200737 as to S3-200738: In clause 5.3.3, its unclear what "all supported data rates" means or implies to the gNB, and we don’t support the proposed update to the gNB in clause 5.3.3 in TS 33.501.

**Current Status: Under Discussion**

**Blockers: Samsung, Qualcomm, Telecom Italia, DT, Broadcom**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200766 On the GSMA LS on UP IP Qualcomm Incorporated, vivo, Nokia, Nokia Shanghai Bell

**[Conf call]** Presented by Qualcomm

**[Conf call] DoCoMo:** The first 2 are ok - but 3rd cannot be agreed

**[Conf call] T-Mobile USA:** I support this document

**[Conf call] Orange:** I don’t want to wait for he LTE solution before having the 5G solution.

**[Conf call] Qualcomm:** We believe that mandating UPIP for all UEs is not acceptable because it may not be appropriate for some services.

**[Conf call] Vodafone:** we agree observation 1 and 2 (for different reasons to Qualcomm) but not 3 (as there are other vulnerable services)

**[Conf call] DoCoMo:** agree with VF but for 3 it will be hard to determine what traffic is DNS.

**[Conf call] Qualcomm:** we are proposing just to protect specific DNS servers (operator managed)

**[Conf call] CableLabs:** Agree with VF (Steve B email), should not be piecemeal.

**[Conf call] Chair:** leave open by email… especially observation 3

**Current Status: Under discussion**

**Blockers: DoCoMo, Vodafone, CableLabs**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200767 Proposed solution for UP IP issues in GSMA LS Qualcomm Incorporated, vivo

**[Conf Call]** Qualcomm presented the document

**[Conf Call] DoCoMo:** Whilst mitigation 1 is possible we think that mitigation 2 will cause problems as various service potentially use ICMP for discovery and keep alive reasons.

**[Conf Call] Vodafone:** We are happy to endorse this paper (at least mitigation 1) as long as it does not exclude the agreement on a full general solution to UPIP.

**[Conf Call] Chair:** We have run out of time for this topic… lets continue this document on email…

**[email] NCSC:** Regarding the use of DNS over TLS (mitigation 1), what kind of DNS are we talking about here? I am interested in whether operators will be able to read requests coming into its DNS server, for the purposes of:

1. Network analytics

2. Blocking requests to forbidden websites

If the DNS request is encrypted, then the operator can’t see it unless they own the DNS server – will the network be providing its own DNS servers for users?

**[email] Qualcomm:** Mitigation 1 is about the use of DNS over TLS between the UE and the operator managed DNS server (only this is within the scope of 3GPP); I believe 1 & 2 should still be possible. Also, note that only integrity protected is needed to mitigate the described attacks for the selected TLS cipher suites. Use of any private DNS by users is outside the scope of 3GPP (as explained in the NOTE in the contribution). My understanding is that operators can (and do in many cases) configure their over DNS servers and the procedures for DNS configuration for a given PDN/PDU sessions are specified in 3GPP.

**[email] CableLabs:** I agree with Qualcomm that 1 (network analytics) & 2 (DNS based filtering) are still possible since the DoT server is controlled by the operator. One operational issue to consider for DoT is that each DoT client must be able to verify the certificate of a DoT server. This would require an operator to issue certificates to its DoT servers and provision DoT clients to trust those certificates. If the support of DoT is agreed, we should also capture DoT certificate related issues.

**[email] Huawei:** I think the comments on using DNS security for S3-200695 are also applicable for this document (S3-200767). My opinion is that the DNS TLS introduced could be taken as one measure to mitigate or even resolve the attack raised by GSMA this time, however, it can’t be deemed as the alternative for the UPIP. It’s better to take the two things separately. We (SA3) shall be much more responsible and cautious on this issue since UP IP is introduced by us in 5G phase, therefore, it’s meaningless that we just address the specific attack case by case.

**[email] NCSC:** I agree with the views put forward by Rong, and by people such as Steve Babbage on other threads, that UPIP support is a better way of protecting against the attacks that we’re worried about. It mitigates against a broader range of attacks than just the ones mentioned in the GSMA LS, and is a simpler solution - meaning that operators don’t have to go and implement DNS over TLS as well – which is generally preferable.

**Current Status: Under Discussion**

**Blockers: Vodafone, NCSC, Huawei**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200629 pCR to TR 33.853 move of network options from introduction to section 4 VODAFONE Group Plc

**[email] Qualcomm:** This pCR should be noted as the existing Introduction clause already provides the necessary background/motivation for the study. The intent of network options clause, as described by the editor’s note, is still valid. If there is no intent to complete this clause, we are ok with removing/voiding this clause.

**Current Status: Under discussion**

**Blockers: Qualcomm**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200635 Cover sheet for TR 33.853 for Information VODAFONE Group Plc

**[email] Qualcomm:** I propose that this be noted. Motivation: There is no SA plenary meeting before our next SA3 e-meeting. We can decide on this at the next SA3 meeting based on TR 33.853 progress then.

**Current Status: Under Discussion**

**Blockers: Qualcomm**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200639 pCR to 33.853 (UPIP) - Correction to Key Issue 5 VODAFONE Group Plc

[email] Qualcomm: We don’t agree with this pCR for the following reasons:

- The key issue #5 is for the support for UP IP as specified in 5GC where there is method to negotiate security policies on a PDN basis. Such a mechanism does not exist for EPS. It is not clear yet whether the same approach will be followed with EPC or a different approach will be followed. Therefore, we don’t agree with updating key issue #5

- Another issue we have is regarding home terminated vs visited network terminated DNNs. For the latter our understanding is that the security policies (including UP IP) are decided by the visited network and not home network. This needs to be taken into account.

Therefore, we would this contribution to be noted. Alternatively, we will also be fine with introducing a new key issue in the TR for this dealing with EPC connected options.

**[email] Vodafone:** The point of this document is to correct clear errors in Key Issue 5.Please provide a revision rather than blocking progress.

The HPLMN is in control of whether a DNN breaks out in the VPLMN, so the HPLMN remains in control.

**[email] Vodafone:** (to bullet point 1) the point is that when Key Issue #5 is documented with a correct description of R15 5GC, it is NO longer an issue for 5GC! But for EPC there is work to investigate…

(to bullet point 2) your understanding does not seem to align with TS 23.501, Figure 4.2.4-4: Roaming 5G System architecture - local breakout scenario in reference point representation (below). In this figure you can clearly see that the SMF in the VPLMN has an N10 interface to the UDM This is the interface that would signal the security policy (e.g. UPIP mandatory) to the VPLMN

[email] Qualcomm: it may very well be the case – I will have to check both stage 2 and 3 relevant text in the specs on this. Unfortunately, I am unable to do this before the close of this e-meeting.

(Vodafone said) The point of this document is to correct clear errors in Key Issue 5.[Anand] I don’t believe it is just correcting errors, it is rather a) modifying the scope of the key issue (which is currently only applicable for 5GC; my proposal is to introduce a new key issue to cover EPC connected options); and b) proposing a way to solve the existing key issue by setting the UP IP policy for the DNN to required – this is a solution and not correcting errors in the key issue description, IMHO

(Vodafone said) Please provide a revision rather than blocking progress.

[Anand] I am sorry that you interpreted my comments this way. FYI, Qualcomm has been actively supporting (co-signer of the SID) and contributing to this study and TR. Also, the norm in SA3 is that the souring companies provide the revisions, not the commenting companies. However, I am willing to work with Vodafone on this before the next meeting (mainly due to lack of time on my part to work on this before this meeting ends).

(reply to VF on bullet 1) please see my reply above. As explained there, it is not correcting description and mixes EPC with 5GC way of security policy handling

(reply to VF on bullet 2) Thank you for the reference. I will check into this later to confirm this, but still, IMHO, this is not correcting errors in key issue description but proposing a new solution, where you propose to set the UPIP security policy to mandatory for each DNN.

**[email] Samsung:** I agree with Anand to note this pCR for this meeting. Proposal does not clear the errors, it introduce new feature: policy from HPLMN to decide UPIP. This proposal here can be a new key issue for considering HPMN policy in UPIP decision making, as there are existing solutions which addresses the Key issue in the current form.

**Current Status: Under Discussion**

**Blockers: Qualcomm, Samsung**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200760 Interworking between EPS and 5GS when UP IP is supported in EPS Qualcomm Incorporated

**Current Status: No Comments**

**Blockers: None**

**Expected Status at end of meeting (unless there are further comments): Approved**

# S3-200636 minutes of UPIP confcall #1 on 2 April 2020 VODAFONE Group Plc

**[email] Vodafone(Rapporteur):** As these are minutes of a previous conf call and are for information only, Vodafone Propose to **Note** this document

**Current Status: Proposal to Note this document**

# S3-200637 minutes of confcall 2 on UPIP held 3 April 2020 VODAFONE Group Plc

**[email] Vodafone(Rapporteur):** As these are minutes of a previous conf call and are for information only, Vodafone Propose to **Note** this document

**Current Status: Proposal to Note this document**

# S3-200634 LS to RAN3 and CT1 on Updated User Plane Integrity Protection advice VODAFONE Group Plc

**[email] China mobile (Vice Chair):** The contribution should be revised to remove all description related with Rel.17.

**[email] Telecom Italia:** could you kindly provide the the rationale behind your request?

**[email] China Mobile (Vice Chair):** The rationale is very simple. What we are talking now is about Rel.16 and all we need to solve is Rel.16 issue. All Rel.17 material is not related to this release.

**[email] Qualcomm:** Qualcomm does not agree with this LS proposal. As being discussed in various other contributions/threads, it is clear that there are different proposals on how to address the threats identified in the GSMA LS. I think we need to conclude on those proposals first before discussing any potential LS to other WGs groups on this topic.

**[email] Vodafone:** China Mobile, your reasoning makes no sense to me. If we want to communicate something about R17 to another group, then we can do so. There is no rule preventing us from doing so.

**[email] China Mobile (Vice Chair):** Then the contribution makes no sense to the meeting. It does not follow the meeting motivation. The meeting is used to make sure we finalize our work in release 16 and allow enough time for stage 3 work as well. What is more, if you insist on involving Rel.17 material, please correct the coversheet as it mistakenly shows related release is 16. That will make people confuse.

**[email] Vodafone:** The meeting objective for this study item is to “Progress work on FS\_UP\_IP\_Sec in particular for option 2”. It doesn’t say “exclusively for option 2”, and it doesn’t say “exclusively for R16”. Does anyone else agree with Minpeng’s view that a LS from this meeting shouldn’t even be allowed to mention R17 as well as R16? I just can’t see any justification for this restriction. As for the cover sheet: the draft LS mentions both R16 and R17, so what do you recommend? Are we allowed to list multiple releases? If not, then associating it with the earliest affected release seems sensible to me.

**[email] China Mobile (Vice Chair):** I think we need clarification from Mr. Chair now. The argument comes from the statement when Mr. Chair triggered this meeting. And I don’t see any necessity to discuss R17 topic for only one study item but without other R17 WIs/SIs.

**[email] Chair:** In my understanding this is business as usual and there are no restrictions for which releases to mention in the discussions. You are free to discuss proposals for any releases. In the end we still need to agree on a WID for that release to be able to introduce any changes in the specs unless the release is frozen. IMHO for this study, we still have time for Release 16 and we should focus on that. OTOH it is not at all uncommon that during studies, agreements are made for example to address key issues or push features to future releases. In case there is consensus on an action for Release 17 then that is fine by me, we will minute that and we are not breaking any rules. However as I said above we still need consensus on a WID. If there is no consensus on actions for Release 17, I invite you to express your objection. I have neither the means nor the intention to stop anyone from writing their views. Let’s not spend more time on this discussion.

**[email] Telecom Italia:** honestly I tend to agree with Steve.

Since the 5G “options” are a reality, SA3 would probably like to address the “UP IP” issue for all “options” within Rel-16 timeframe.

Having a FS\_UP\_IF started in Rel-16 could perhaps confirm such a willing.

However it looks probably too much optimistic to assume that this will really be possible, for all “options” within the (almost expiring) Rel-16 timeframe. For “Option 2” SA3 was prompted by SA to do it for Rel-16, however it sounds very reasonable (to me, at least) that SA3 will have the chance to address the remaining “options” within Rel-17 timeframe.

Also because some of the remaining “Options” are expected to be deployed earlier than Option 2, in many Countries (e.g. Option 3) and for the remaining “options” it would not make sense to address the UP IP issue in Rel-18, or Rel-19.... Isn’t it? Moreover, a LS is a LS, it is not a TS carved in the stone... A LS does not have normative value and in my view it does not harm to take the opportunity of this LS to inform other WGs about the intentions of SA3, especially now that Rel-16 is basically over and that Rel-17 work is officially ongoing (even if most agenda items started for Rel-17 are around their 0% ... ) They would be warned in advance, and hopefully will not need to be in a rush, to progress or amend their TS due to UP IP issue.

**[email] Ericsson:** Ericsson has a concern about the statements/requirements in the LS in S3-200634 regarding the gNB, (ng-)eNB and en-gNB. For the gNB, its very unclear what the following statement/requirement “UPIP shall be supported by … the gNB … regardless of the data rate from Release 16 onwards.” implies or means to the gNB in bullet 1. We have the same comment to the (ng-)eNB and en-gNB in the other bullets. So the requirements related to the gNB/(ng-)eNB/ en-gNB in the LS, are not acceptable to Ericsson.

**[email] Qualcomm:** Just for the record, in case it is not clear already, Qualcomm requests that this contribution be noted. This is related to our discussions on UP IP way forward as well as S3-200631, both of which has not been concluded.

[email] China Mobile: I see the discussion is divided into two threads so I’d like to make my comments here to keep it back to one thread.

For Monica’s comment, the statement follows the discussion on threads about S3-200643(way forward from Futurewei) and S3-200633(CR from VF). I think it is quite clear.

For Mauro’s comment, I’m not objecting any options study nor objecting any solutions for any options. I totally agree with you that SA3 needs to address the issue in other options and we have time in R17. What I concern is mainly happened in this meeting. It is too early to make such statement for R17. Although I’m fine with the motivation to have UP IP mandatory for other options in R17, we could not make such strong statement without any mature solution.

For Mr. Chair’s comment, the points I get are no restriction for releases but we should focus on R16. I will follow this way for further discussion in this meeting although I have a little bit confuse still.

For Steve’s comment, the comment for content can refer to the response to Mauro’s comment. For coversheet issue, the easiest way is to list R16 & R17 together but I’ve no idea whether this is follow the rule of document template. It needs to be checked with Mirko. The other way is also quite simple as the LS can be divided into two LS. One is for R16 only and the other is for R17.

**[email] CableLabs:** Thanks for the merging the discussion and summarizing the comments. I think this LS is well written which clearly describes the potential risk from the lack of UP IP in full data rate and outlines the SA3 position as a security group. We support to send this LS out.

**[email] Huawei:** Thanks Minpeng to collect the opinions and it’s convenient to focus on the most important thread because actually we are quarrelling about the same thing. I would like to say from security perspective, Huawei support that UP IP shall be supported without data rate limitation. In this case, we don’t need to explain the same types of attacks because of lack of UP IP again and again. And this is addressing the original GSMA LS and SA plenary request I believe. Considering the time being, I think for Option2, SA3 shall identify the potential changes as soon as possible to make it in R16 timeframe. The time is very limited. It requests not only SA3, but also RAN2,CT1,SA2 to recognize potential improvement for their specs. For other options, I think the implementation in standard will take much longer time, likely in R17 timeframe. But in my understanding, the original intention is to mandate UP IP at full data rate, while in the LS it states “regardless of the data rate” in bullet1,2,3,4. Do we request the full data rate or any data rate for UP IP exactly? If we are not clear on this point, it will cause confusion to other groups, especially in RAN2 and CT1. I would like to remind, if SA3 would like to proceed this issue further, a LSout on Option2 issue to other relevant group is very necessary for this meeting, otherwise, it can’t catch up with R16 pace.

**Current Status: Under discussion**

**Blockers: Qualcomm, China Mobile, Ericsson**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200738 Draft LS on UP IP Huawei, Hisilicon

**[email] Telecom Italia:** Based on the comments raised against S3-200737, Telecom Italia does not support this contribution.

[email] Ericsson: Ericsson has the following comments to S3-200738. The LS states:

"SA3 endorsed the requirement that the UE and network shall support user-plane integrity protection and replay protection of user data for all supported data rates."

We think the part about the network (marked with yellow colour above) should be removed from the sentence above copied from the LS. Its unclear to us what "all supported data rates" means for the network.

There is already a requirement in TS 33.501 which states that the gNB shall support UP integrity protection, which is sufficient.

**Current Status: Under discussion**

**Blockers: Telecom Italia**

**Expected Status at end of meeting (unless there are further comments): Noted**

# S3-200630 pCR to TR33.853 (UPIP) - Addition of conclusions to section 7.2 VODAFONE Group Plc

**Current Status: Withdrawn**

# S3-200638 Discussion document on the approval of TR33.853 VODAFONE Group Plc

**Current Status: Withdrawn**