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

Date: 15/04/2020 @ 23:00 UK Time (BST)

Version: 3

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| S3-200630 | pCR to TR33.853 (UPIP) - Addition of conclusions to section 7.2 | Final Status  **Withdrawn** |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**

# 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)]

**Current Status: under discussion**

# 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.

**Current Status: Under Discussion**

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

**Current Status: No Comments**

# 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.

**Current Status: Under discussion**

# 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.

**Current Status: under discussion**

# 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.

**Current Status: under discussion**

# 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:** 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.

**Current Status: under discussion**

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

**Current Status: No Comments**

# 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).

**Current Status: Under discussion**

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

**[email] Hauwei:** 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**

# 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.

**Current Status: Under Discussion**

# 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).

**Current Status: Under discussion**

# 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

**Current Status: Under Discussion**

# 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**

# 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**

# 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**

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

**Current Status: No Comments**

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

**Current Status: No Comments**

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

**Current Status: No Comments**

# 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.

**Current Status: Under discussion**

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

**Current Status: No Comments**

# 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**