**3GPP TSG-SA3 Meeting #99Bis-e *Draft 3 S3-201429***

**e-meeting, 11-15 May 2020**

**Source: Vodafone (Rapporteur)**

**Title: Minutes of UPIP discussion in SA3 #99**

**Document for: Information**

**Agenda Item: 5.9**

Rapporteur's minutes for UPIP in SA3 99e

Date: 20/05/2020 @ 11:30 UK Time (BST) Version: 9

# Summary:

| Document | Title | Outcome\* | Revised Doc Number |
| --- | --- | --- | --- |
| S3‑201008 | UP IP-new solution on UP security policy activation | Noted(Huawei, Nokia, Ericsson) | - |
| S3‑201031 | CR to 33.501 - Update to User Plane Integrity Protection | Noted(Samsung, OPPO, Qualcomm) | - |
| S3‑201142 | Revise the Evaluations for Solution 5 in TR 33.853 | Noted(Qualcomm, Nokia) | - |
| S3‑201206 | LS to SA2 and RAN2 on questions of UP IP | Noted(Samsung, Ericsson) | - |
| S3‑201207 | Modification on the Key issue #3 for UP IP | Noted(Qualcomm) | - |
| S3‑201208 | UPIP: pCR for new solution to address UP IP support at full data rate | Noted(Qualcomm) | - |
| S3‑201209 | UP IP: Conclusion for Key Issue #3 | Noted(Qualcomm) | - |
| S3‑201274 | Security Aspects of DNS and ICMP | Email Approval as S3-201392 \*\* | S3-201391 |
| S3-201391 | Security Aspects of DNS and ICMP (revision of S3-201274) | Email Approval(version 2) | - |
| S3‑201275 | Security Aspects of DNS and ICMP | Email Approval as S3-201391 \*\* | S3-201392 |
| S3-201392 | Security Aspects of DNS and ICMP (revision of S3-201275) | Email Approval | - |
| S3‑201295 | Protection of DNS messages | Noted(Huawei) | - |
| S3‑201296 | UP integrity protection for UP Signalling messages | Noted(Huawei, Ericsson) | - |
| S3‑201297 | Integrity Protection for UP Signalling messages | Noted(DT, Futurewei) | - |
| S3‑201298 | Conclusion to Key Issue #5 | Noted(Huawei) | - |
| S3‑201305 | pCR to TR 33.853 (UPIP): addition of new solution - use NR PDCP for LTE | Approved | S3-201427 |
| S3‑201307 | LS to RAN2 and CT1 on Updated User Plane Integrity Protection advice | Email Approval(version 3) |  |
| S3‑201310 | Cover sheet for TR 33.853 for Information | Approved | (no revision needed) |
| S3‑201314 | pCR to 33.853 (UPIP) - Correction to Key Issue 5 | Approved | S3-201421 |
| S3‑201317 | Reduced overhead for UP IP for 5G RAN updates and conclusion | Approved | S3-201366 |
| S3‑201318 | Draft TR 33.853 v0.8.0 | Approved | (no revision needed) |
| S3-201429 | Rapporteurs minutes for UPIP (agenda 5.9) (This document) | Email Approval(version 3) | - |
| S3-201430 | Draft TR 33.853 v0.9.0 | Email Approval | - |

\* Brackets show the confirmed objectors.

\*\* These documents have been put to email approval after they were issued new document numbers. Please comment using the new document numbers.

Don’t forget the WID (S3‑201308 - draft WID - Normative changes for UPIP - VODAFONE Group Plc) **in agenda item 4.27** (Now added at the end of this doc)

|  |  |  |  |
| --- | --- | --- | --- |
| S3‑201308 | draft WID - Normative changes for UPIP  | Email Approval(Version r1) |  |

Detailed Minutes (from emails and conf calls (where held)):

|  |  |  |
| --- | --- | --- |
| S3‑201008 | UP IP-new solution on UP security policy activation | Apple |

[Huawei]The proposed solution recommend the UP security policy activation granularity to be the DRB level which was abandoned when we were specifying the mechanism for TS 33.501.

Now you can see, the current specification supports the PDU Session level. We had a lot of discussion on the granularity.

Since it’s already accepted and standardized clearly in TS, we don’t need to reopen this struggle again. The DRB level based solution now will bring big impact on the current architecture, not only SA3, but also SA2.

So we are not fine with the proposal.

[Apple] May I ask what is the reason to abandon the DRB level granularity?

[Huawei] The main reason is the SMF from network side is not aware the DRB which is the air interface concept. So this kind of security policy can’t be workable actually.

QoS flow, DRB, PDU Session were compared at that time. In the end, RAN2 and SA2 also SA3 determined to choose PDU Session granularity.

If you are interested, maybe you can check the exchanged discussions last year or the year before last year.

[Apple] We are working on new solutions to solve the UP IP supporting issue, in case that full data rate is not supported, there should be more choice to make the capability limited UE to enable finer granularity security configuration in DRB level.  Your concern can be added in the evaluation part, which is, the SMF will be impacted.

[Nokia] I agree with Rong, this proposal changes lot of current concepts and I do not see a benefit either, the UP IP policy is applied anyways at the DRB level. But SMF being aware of every DRB, we are past that discussion.

[Apple] The benefit is UE can configure the UP IP more flexibility when the full data rate can not be enabled. The past discussion is past, we have to look forward, as I said, the impact to SMF can be added as the part of thew evaluation.

[E///] Ericsson has the same view as Nokia and Huawei

**Blockers: Huawei, Nokia, Ericsson**

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

##

|  |  |  |
| --- | --- | --- |
| S3‑201031 | CR to 33.501 - Update to User Plane Integrity Protection  | Deutsche Telekom |

[DT] As I had spotted missing Word change bars in my document (S3-201031.docx), there shall be soon a revision available in drafts folder, named S3-201031-r1.docx that has change bars enabled.

[E///] About the new requirements related to the gNB, we think that the CR in S3-201031 goes beyond what GSMA is asking for. We already have the requirement since Rel-15 that gNB shall support full rate UP IP.

The intention with this contribution seems to be to introduce new requirements on the gNB in Rel-16, because of the following requirement:

*The gNB shall support integrity protection and replay protection of user data between the UE and the gNB for all supported data rates.*

It’s not clear to us why ‘*for all supported data rates* ‘ needs to be added to the gNB and what it implies in terms of hardware? This requirement may have impact on existing gNB nodes.

RRC/NAS encryption and integrity protection support do not mention data rate on network side, and we believe that it should be kept same way for UP integrity protection.

If the requirement about ‘*for all supported data rates* ‘ on the gNB in clause is removed from S3-201031, then S3-201031 is acceptable to us.

[Telecom Italia] Telecom Italia would like to support S3-201031-r1.

[DT] Thank you very much for your feedback “We already have the requirement since Rel-15 that gNB shall support full rate UP IP.” With that clarification I agree to your proposal:

To remove ‘*for all supported data rates* ‘ on the gNB in clause from S3-201031.

[Qualcomm] Qualcomm position is that this CR **shall not be pursed.** Our rationale for this position is documented in S3-200766. Furthermore, this topic has been discussed extensively at SA3#98-Bis-e meeting. I don’t think it is very fruitful to repeat the same arguments again here.

[Spreadtrum] I do not think It is reasonable of removing ‘for all supported data rates ‘ on the gNB in clause from S3-201031. Actually, the rationale about gNB from Ericsson can be applied to UE as well:

*“It’s not clear to us why ‘for all supported data rates ‘ needs to be added to the gNB and what it implies in terms of hardware? This requirement may have impact on existing gNB nodes.”*

If the network and the UE cannot be aligned for UPIP, UPIP will be a meaningless feature.

[Secretary] Some comments on my side:

* Missing “S3” on Source to TSG on the cover page.
* Work item code is wrong. A study can never generate normative work (like this cat-C CR). This will have to be TEI16. And SA will not like it since we need WIDs even for small changes. Otherwise, this work cannot be tracked in the future.

NOTE 2 in clause 5.3.3. is normative. I suggest to make it plain text to keep the requirement.

[Vodafone (Rapporteur)] There is a normative WID for agreement at this meeting for changes due to UpIp  ( S3‑201308)

[Secretary] Sorry, I missed that. I was going to check all WIDs and SIDs after the CRs.

In that case, I suggest to use the WID code “UPIP\_SEC” and write in the “other comments” field that this CR is to be sent together with the normative WID. Noamen should write it down for his presentation to SA.

I will comment separately on the WID, but looking at 308 it needs to refer in its objectives to the work with GSMA, not just the TR in 33.853.

**[DT]** I’ve updated the document according to the comments and uploaded the new version <draft\_S3-201031-r3.docx>.

[Samsung] More or less I am repeating the comments I made in the last meeting.

**Comments:**

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? As the CR claims it address the GSMA referenced attacks in the reason for change.

3) I support Tom (Spreadtrum)comments on UE and gNB requirements. Why the requirement on the UE and the gNB has different interpretation in TS 33.501?

 **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.

**[oppo]** This is Jianhua from OPPO, we share the concerns from Qualcomm and Spreadtrum that we have a extensively discussion on this issue in the last meeting and no conclusion on the pros and cons, and we think it is not fruitful to debate again in this meeting. One possible way we can accept is to introduce more values as proposed in S3-201297 by Samsung, thanks.

[Futurewei] I am sorry but we have to remove “for all supported data rates” in the CR.  It was reluctantly reasonable two years ago when UPIP was discussed, it is no longer reasonable now. But SA3 and the RAN groups made a conscious decision two years ago due to device availability.  That was two years and I would not like to have another conversation two years down the road. If you support many data rates, you are creating many classes of UEs with different security capabilities.  This is not acceptable. UPIP is a distinguishing feature of 5G security.  This has to be supported NOW, not later.

I do not accept introduce more values.  It is not as simple as more values.  More values of support means UEs have different security capabilities.  When you introduce UEs with different security capabilities in the network, you are creating a security problem for the network.

[Nokia] The current specifications in 33.501 allows for integrity protection of all data rates supported by the UE. The same is true for gNB as well. From the discussions it is clear that, there is resource dependency on both gNB and UE, and UP IP need to be enabled based on the APN policy and application.

The assumption that, all UEs operating at full rate with UP IP enabled is not correct and not practical.

I think   complimentary solutions proposed in #1296 and #1274 should be considered to mitigate the attacks mentioned by GSMA.

[Telecom Itlia] In regard to the support of UPIP, TS 33.501 did not put any “rate limitation” to the gNB, nor to the UE, since ever. This lack of “rate limitation” was implicitly intended to be, at least within SA3, that UP IP needs to be supported regardless of the “rate”.

I do not want to repeat here the whole history that brought SA3 to this never ending discussion, however it is evident that SA3 should try to conclude and, really, close this issue...

Possibly also taking int account what MNOs are asking for....

Regardless of possible “**tailored workarounds**” (mostly supported by some Vendors), to be studied, invented and then specified in 3GPP “on the fly” **to counteract the latest precise attack reported by GSMA**, most **MNOs clearly expressed their need and clear preference for a future proof, more “general purpose” solution**, that would be effective also for similar (but different) new attacks that could easily be exploited in the future (without the need of a new “tailored workaround” on the fly....).

**MNOs believe that such a future solution is the UP IP supported up to the maximum supported rate**. And they would like to have it. Moreover MNOs are not willing to fragment the ME market legitimating various “rate limitations”.

I am really struggling to understand why Vendors are not willing to support what their customers want, for the UP IP...

Telecom Italia can accept a possible “**tailored workaround**” to counteract the precise attack reported from GSMA, if Vendors really want it, **as long as the tailored workaround does not rule out the future proof, general purpose solution**.

To me, being “complimentary” (as Nokia wrote in the previous email) means that there is an alternative to the tailored workaround and since we are discussing SA3-201031, I hope that such an alternative is the future proof, general purpose solution that MNOs asked, and still ask, for: the UP IP supported up to the maximum supported data rate.

 Telecom Italia was fine with S3-201031-r1 where *“for all supported data rates.”* was explicitly added for the gNB.

Ericsson claimed that such an addition is **not needed for the gNB** since (their?) gNBs do not have any rate limitation, since ever...

**If SA3 is sure that all Vendors are in the same position as Ericsson for the gNB**, then I can accept Ericsson objection and S3-201031-v4 (even if I still fail to understand why S3-201031-v1 could harm whatsoever gNB vendor), otherwise I think that S3-201031-v1, with  would be preferable (to avoid future mis-interpretations and re-start this unbelievable discussion..)

[Ericsson] I have not been able to follow all the discussions on UP IP, so I am not up to date on the discussions taking part, but I just want to clarify that our comments and concern that we raised was more related to if RAN2 decides to introduce new maximum data rates in Rel-16 or later releases. Our view is that we don’t need this requirement *“for all supported data rates.”* for the gNBin our specifications.

[Vodafone] To be clear: you say we don’t need that text, but does it do any harm?  Is your comment a blocker to approval?

[Telecom Italia] I think that the addition of *“for all supported data rates.”* for the gNB (as in S3-201031-r1) would not harm, but **if Vendors can guarantee that no one gNB worldwide has “rate-related” issues for UP IP**, then I would be fine also with S3-201031-r4, where *“for all supported data rates.”* is removed for the gNB.

[Ericsson] Ericsson is willing to agree the CR if *“for all supported data rates.”* is removed from the gNB as proposed in 201031-r4.

[Nokia] Nokia has issues with the current wording in r4.

What does the new sentence mean ‘The UE shall support integrity protection and replay protection of user data between the UE and the gNB at the UE’s maximum supported data rate.‘ Is the UE and the gNB expected to support maximum data rate support for UP IP at all times?

The new  NOTE2 is clearly in contradiction to the security policy per PDU session sent by the AMF. What is the intention of the NOTE and how does it co-exist with AMF policy per APN?

[Spreadtrum] I fully understand your concerns. But the question is how **Vendors can guarantee that no one gNB worldwide has “rate-related” issues for UP IP.** Sincewe are discussing in 3GPP, we have to consider what is in the 3GPP scope.

[Telecom Italia] gNBs are supposed to be 3GPP elements therefore I think they certainly are within the scope of 3GPP.

Maybe not all Vendors available worldwide attend 3GPP meetings, and this is why I would have a slight preference for S3-201031-r1 (since in my view the addition of *“for all supported data rates.”* for the gNB) would not harm.

But if Vendors attending 3GPP meetings agree with Ericsson and prefer S3-201031-r4, I am fine too.

[Spreadtrum] My point is that 3GPP specification(s) are the place for such guarantee, otherwise I would like to suggest to at least document such statement in the meeting minutes: **Vendors(E///, ...) can guarantee that no one gNB worldwide has “rate-related” issues for UP IP.**

**Blockers: Samsung, OPPO, Qualcomm**

**Status at end of meeting (unless there are further comments): Not Pursued**

|  |  |  |
| --- | --- | --- |
| S3‑201142 | Revise the Evaluations for Solution 5 in TR 33.853  | China Mobile |

[Qualcomm] Though header compression (i.e., ROHC) is supported at the PDCP layer, it’s not usually or always configured. Header compression is typically configured for the bearer of voice traffic where the header size is relatively big compared to the payload size.

Considering that ROHC is optionally configured, Qualcomm don’t think the proposed changes are sufficiently justified. For most of the traffic, the existing evaluation still applies.

Therefore, we propose to **NOTE** this document.

[Nokia] The change in the ‘Compatibility’ part is not correct. Just Integrity Protecting only the header part is something new for PDCP, it need changes at PDCP layer, not compatible without specific changes to support it.

[China Mobile] I would like to make some clarification for this topic.

ROHC is mandated to support, and optional to use. To implement ROHC,  the PDCP layer has to first identify the type of packets. ROHC can be not only applied to the bearer of voice traffic, but also the bearer of some other kinds of traffic.

To support header integrity protection, we can activate the ROHC or activate only the function to identify the type of packets. In a nutshell, ROHC is supported at the PDCP layer, which can be used to identify the type of packets. ‘Compatibility’ part could be revised according to Suresh’s comments.

**Blockers: Qualcomm, Nokia**

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

|  |  |  |
| --- | --- | --- |
| S3‑201206 | LS to SA2 and RAN2 on questions of UP IP  | Huawei, Hiliscon |

[Samsung] Samsung propose to Note this LS. As the questions are for clarification and for solution considerations in later releases (not for Rel-16), it can be considered in the upcoming meetings.

[Nokia] We do not see the need for this LS. The answers to all the three questions are clear in the current specifications, we do not see these questions clarifying anything further.

[Huawei] The Q2 and Q3 are related to later release, but Q1 is related to R16. The intention of Q1 is trying to get some clarification and could make SA3 know what’s the limitation of integrity protection maximum data rate on activating UP IP, and we think this is useful for our understanding and progress.

If there is no agreed LS in this meeting, this is no harm to send this one, and we can leave the Q2 and Q3 out if you think there are not needed.

If there is an agreed LS, we can merge Q1 into the agreed LS.

[Ericsson] Ericsson does not see the need to send the LS in this meeting as it mainly relates to Rel-17 scenarios which are still studied.

**Blockers: Samsung, Ericsson**

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

|  |  |  |
| --- | --- | --- |
| S3‑201207 | Modification on the Key issue #3 for UP IP  | Huawei, Hiliscon |

[Qualcomm] This contribution shall be **noted**. The key issue #3 was introduced in the TR to specifically study the ways of achieving full data rate UP IP in the up link while also meeting the latency requirements of use cases where ultra-low latency is expected. This is because, in NR, the scheduling on the uplink is controlled by the gNB and depending on the QoS requirements, the UE must respond within the grant time on the up link.  This is not a problem on the downlink as such a restriction does not exist. Therefore, we don’t agree with the modification of the KI proposed in this contribution.

[Huawei] Is there any security reason on only integrity protect the uplink user plane data, without integrity protect downlink user plane data? It’s strange. We need to care about the uplink and downlink. If you apply DRB IP, then both uplink and downlink user plane data will be integrity protected, do you want to separate them? Or do we have to add a new key issue specific for downlink data protection?

[Qualcomm] My point was different. Yes, we should be able to integrity protect both uplink and downlink. However, due to asymmetric nature of NR, the data rates for uplink and downlink may be different. However, key issue #3 is to study UP IP optimizations for the uplink so that full data rate can be achieved while at the same time meeting the strict ultralow latency requirements of certain uses cases– Uplink UP IP is challenging in in this case (i.e., very high data rate and ultralow latency) as the UE does not control scheduling of the uplink (thus the time available to perform UP IP for all up link packets).

As I stated below, this time constraint for the UP IP packets doesn’t exist at the UE for the downlink. This is why this key issue is only about the uplink and not the downlink

**Blockers: Qualcomm**

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

|  |  |  |
| --- | --- | --- |
| S3‑201208 | UPIP: pCR for new solution to address UP IP support at full data rate  | Huawei, Hiliscon |

[Samsung] Question for clarification: What is meant by "eMBB or URLLC UE" and How a UE knows it is "eMBB or URLLC UE".

[Vodafone] I don’t mind whether that text about “eMBB or URLLC UE” is included or not – it is clearly only there for motivation, giving examples of cases in which 64kbps is not fast enough.

On the contribution as a whole, though, it seems quite clear that “Support of UP IP at full data rate for Option 2” is a valid solution that should be included in the TR.  Whether you choose to progress it is another matter, based on evaluation … but it’s a valid solution.

[Huawei] I agree with Steve, this is just an example. If you insist to clarify, I can make the solution more general, like “for ~~eMBB or URLLC~~ most of UEs”

Do you agree with that?

[Samsung] Better to have EN than changing it to "most of UEs". '

EN: Definition of "eMBB or URLLC UE" is FFS

[Huawei] We already have a NOTE in the solution. And we think this should be defined in RAN or CT.

So, how about adding some description in the NOTE?

NOTE: The support of UP IP at full data rate impacts RAN and CT standardization. Therefore, the relevant RAN WGs and CT WGs need to be consulted once this solution is adopted. For example, definition of type of UEs.

[Samsung] Updated Note is fine with me.

[Qualcomm] I don’t think definition of UE category based on its categorization such as eMBB UE or URLLC UE are in the scope of SA3 or even 3GPP. If you think it is, could you please provide reference to where such categorization is defined in 3GPP?

I also, this can’t be a solution to key issue #3 (as I have explained the motivation behind  Key Issue #3 in the thread on S3-201207)  - i.e., there is no key issue to study this in the TR.

Therefore, this document should be noted for this meeting.

[Huawei] eMBB and URLLC are already modified to "most of UEs”, the idea is some of categorization should be defined in other group.

Even modification of key issue #3 is not agreed, the solution could also address the key issue #3, could you please state why this solution does not work for Key issue 3’s security requirement?

[Qualcomm] This solution relies on UE categorization, which is not in the scope of neither SA3 nor 3GPP. I still request this document to be noted.

[Huawei] I think only you don’t think 3GPP can define that, Samsung and VDF are OK to capture this in NOTE, that means they think RAN or CT could define that.

In this case, how about turning the NOTE to editor’s note since it’s just a solution for SID?

**Blockers: Qualcomm**

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

|  |  |  |
| --- | --- | --- |
| S3‑201209 | UP IP: Conclusion for Key Issue #3  | Huawei, Hiliscon |

Summary: This pCR should be noted.

Motivation: Please refer to comments to S3-201207 and S3-201208.

**Blockers: Qualcomm**

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

|  |  |  |
| --- | --- | --- |
| S3‑201274 | Security Aspects of DNS and ICMP  | Qualcomm Incorporated |

[Vodafone] This contribution from Qualcomm introduces a normative Annex to TS 33.501, with measures to protect DNS and ICMP.

The “reason for change” states, correctly, that when UPIP is not used, DNS and ICMP may be vulnerable.  But the proposed Annexes recommend security measures for DNS and ICMP irrespective of whether UPIP is used.  Shouldn’t they be rephrased in a conditional way, to say something like “If the UE does not support full rate UPIP, then …” or “if the operator cannot guarantee that UPIP can be applied, then …”?

[Secretary]

* WID code is TEI16, not TEI-16.
* Shouldn’t this CR be part of the new normative Work Item for UP IP in S3-201308? SA doesn’t like cat-B CRs being introduced as TEI16. Just change the WID code to UPIP\_SEC and it will be submitted together with the WID.
* Remove the automatic bullet list in X.3, since this is against the drafting rules.

[Qualcomm] @ Steve,  good comment. I propose to modify X.1 in r1 as follows to take your comment into account:

“This annex specifies security measures to protect DNS and ICMP messages. These security measures are intended when integrity protection over the user plane can not be used.”

@ Mirko,

I implemented your suggestions below in r1.

[Huawei} Do we really need a Normative Annex on this? In my understanding, the document propose the specific measures for DNS and ICMP messages protection, however, they can be protected by other means, e.g. UP IP

So, the better way is to change the Normative Annex to Informative Annex, and delete NOTE2.

[Qualcomm] I think Normative is better – I would be interested to hear any preferences from others.

[Huawei] I would like to ask more question, for the DNS protection, does the UE also need to configure the certificate? My concern is that if there is only single direction certificate is configured, there is still Man in the Middle attack.

[NCSC] NCSC would like to reiterate our position (from last meeting and this meeting) that the measures described in this contribution only protect against a subset of the attacks that UPIP would protect against, and are more complicated to implement, which could lead to mistakes in implementation and more security flaws. We therefore support that this is changed to an Informative Annex and Note 2 deleted.

[DT] ideas as proposed in 274 could only be seen as an interim patch.

While discussing mandatory implementation of UP IP in the UE, I saw requests like "then we must mandate UP IP usage by the network as well".

Why do proponents of patches like 274 (instead of full-rate UP IP) not mandate UE implementation and usage these patches as well, then?

Real world experience tells us: patch + "should" = will not reach the customer

On blocking ICMP: this might be easy for IPv4, but not for IPv6. We should at least consider <https://tools.ietf.org/html/rfc4890>

[Qualcomm] @ James O & Rong, Ok, let’s go with an informative Annex and delete NOTE 2.

@ Rong, For TLS over DNS, client authentication is not required (as only the DNS replies to the client need to be protected) – therefore, no need to configure the UEs with client certificates.

@Stefan, I would be fine with making these measures mandatory, but as you very well know, we have to go with SA3 consensus (which currently seems to be leaning towards an informative annex). Yes, we can add a reference to RFC 4890 for ICMPv6 for installing filters.

@ all, I have uploaded r2 to the drafts folder incorporating these comments. Please have a look.

[Samsung] If we progress the work with application layer protection, then parameters required for DNS server authentication needs to be configured in the UE. The configuration parameters are proposed in S3-201295. I provided an update in r3 and uploaded. Please have a look.

[Huawei] I’m fine with r2.

[Qualcomm] Thanks. Please note Samsung uploaded r3. Please kindly take a look and indicate whether r3 will be acceptable to you.

[Huawei] Is there any difference between r2 and r3? Maybe Samsung uploaded the wrong version.

[Samsung] Our update is inclusion of 2 lines at the end of the first paragraph in clause X.2.

[Ericsson] About the following text:

*Install IP filter(s) at the UPF in order to block ICMP messages. This filter can be configured either on a per UE basis or on a UPF basis. For ICMPv6, the recommendations in RFC 4890 [zz] can be used for filtering ICMPv6 messages.*

Maybe we don’t want/need to configure the ICMP filters dynamically from SMF, it can probably just be preconfigured in UPF and possibly activated from SMF.

So maybe using “activated” instead of “configured” would allow more freedom for CT4 when defining the protocol to choose best method (e.g. dynamic filters or just a flag for activation). Would the following update be acceptable to you as follows?

*This filter can be activated either on a per N4 Session or on a UPF basis.*

[Qualcomm] Yes, that would be fine by me. I am still awaiting confirmation from Rong on whether r3 is acceptable to her. I will add this update to either r2 or r3 depending on her confirmation.

[Vodafone (Rapourteur)] 18/May/2020 - At the explicit direction of the chair, this document is now sent for email approval as Huawei had not explicitly accepted r3. Document number is S3-201392.

**Blockers: None**

**Status at end of meeting (unless there are further comments): Email Approval**

**Revised to : S3-201391**

|  |  |  |
| --- | --- | --- |
| S3‑201391 | Security Aspects of DNS and ICMP (revision of S3-1274) | Qualcomm Incorporated |

[Vodafone (Rapourteur)] 18/May/2020 - At the explicit direction of the chair, this document is now sent for email approval as Huawei had not explicitly accepted r1.

Email approval deadlines

•      Doc available:              18th of May      15:40 UTC

•      Comments:                  20th of May      15:00 UTC

•      Final version available: 21st of May      15:00 UTC

•      Approval:                     22nd of May      15:00 UTC

[Huawei] I’m fine with r1 if you can correct as below:

“Clause X (Informative)

Security measures specified in Annex X of TS 33.501 [43], can be used to protect the DNS and ICMP messages that are carried over the user plane.”

[Huawei] The S3-201391 actually was S3-201274. The title needs to be corrected.

Then, for the S3-201391, the sentence “The SMF can configure the necessary DNS server security information (out-of-band configurations specified in the IETF RFCs like, credentials to authenticate the DNS server, supported security mechanisms, port number) in the UE via the AMF. DNS server security information can be provided to the UE along with the DNS server IP address configuration.” shall be removed, because the configuration is UE implementation. For example, the CA certificate is pre-configured in UE’s OS or browser. There is no need to configure it by 3GPP network.

In addition, if 1392 refers to 1391, the text in the 1391 should avoid mentioning 5GC NE. For example, rename UPF to be UP gateway.

[Samsung] UE implementation specific configuration is not correct. More specifically, it is incorrect for, MNO self signed certificates and also when raw Public key is used (both are allowed by RFCs).

There is need for configure it by the 3GPP network. Handling of configuration is implementation specific, but provisioning of the configuration is not implementation specific, as DNS server(s) are deployed by the 3GPP network. Specifically "It is recommended that the UE and DNS server(s) support DNS over (D)TLS as specified in RFC 7858 [xx] and RFC 8310 [yy]. "

Without information from the network, how the UE knows whether to use TLS or DTLS or not to use any protection.

Further how to enforce the text in the CR "The DNS server(s) that are deployed within the 3GPP network can enforce the use of DNS over (D)TLS. ",

You comment on impact to network is incorrect, as all these information can be transferred as part of PCO, which is transparent to the network entities.

We have serious concern, if the network does not provide configuration, then the UE might be in out of service, particularly in roaming scenarios with local breakout or GSMA referenced attack on DNS is possible, if the UE does not use application layer protection due to lack of configuration even though the 3GPP network supports application layer protection for DNS.

[Huawei] We don’t think the MNO may sign certificate using raw Public key instead of certificate, and we don’t think the solution can work if the DNS server is deployed by 3rd, not MNO, neither.

But In order to make progress, how about revising as below:

“It is recommended that the UE and DNS server(s) support DNS over (D)TLS as specified in RFC 7858 [xx] and RFC 8310 [yy]. The DNS server(s) that are deployed within the 3GPP network can enforce the use of DNS over (D)TLS. The UE may pre-configure DNS server security information (out-of-band configurations specified in the IETF RFCs like, credentials to authenticate the DNS server, supported security mechanisms, port number, etc.), or the core network may configure the DNS server security information to the UE.“

We just make the text more general, because this is an informative clause, and 1392 also cite 1391, for 1392, LTE has no NEs named SMF, AMF etc.

[Samsung] Thank you for the revised text. The revised text below is fine with us. I updated the same in r1 and uploaded it to the draft folder.

[Huawei] I don’t know actually whether we already passed the email comment deadline.. But I still would like to say I’m fine with r1.

[Qualcomm] I am also fine with r1, but there were some editorials in the text that was added (e.g., use of “may”) that needs to be corrected.

With these editorial changes, r2 is in the drafts folder. I assume this is also fine with everyone – please indicate otherwise.

**Blockers: None**

**Expected Status after email approval (unless further comments): Approved**

|  |  |  |
| --- | --- | --- |
| S3‑201275 | Security Aspects of DNS and ICMP  | Qualcomm Incorporated |

[Secretary] Same comment as in 274. Better to fit this into the new WID for UP\_IP in tdoc 308. So add the WID code UPIP\_SEC and note to Noamen that this should go together with the WID.

SA is not keen on introducing untraceable new features in the big TEIX basket.

[Huawei] In case the Normative Annex is changed to Informative for S3-201274, the text added here needs to be modified accordingly.

[Qualcomm] Yes, I agree to revise this document based on the outcome of the same comments in S3-201274.

Please find r1 in the drafts folder now. The only changes are to the cover page of the CR to incorporate Mirko’s comments. Please have a look and let me know whether it is acceptable.

[Vodafone (Rapourteur)] 18/May/2020 - At the explicit direction of the chair, this document is now sent for email approval as Huawei had not explicitly accepted r1. As New document number has already been assigned for this, discussion continues in S3-201391.

**Blockers: None**

**Status at end of meeting (unless there are further comments): Email Approval**

**Revised to : S3-201392**

|  |  |  |
| --- | --- | --- |
| S3‑201392 | Security Aspects of DNS and ICMP (revision of S3-1275) | Qualcomm Incorporated |

[Vodafone] This document is on email approval…

Email approval deadlines

•      Doc available:              18th of May      15:40 UTC

•      Comments:                  20th of May      15:00 UTC

•      Final version available: 21st of May      15:00 UTC

•      Approval:                     22nd of May      15:00 UTC

[Huawei] We are fine with r2, not fine with r3. I think this time we can take r2 for the time being.

[Samsung] We are not fine with r2 and we are fine with r3.

With r2 as it is, the UE may go out of service, if the UE does not know whether to use normal DNS request or DNS over DTLS?, for the DNS server IP address provided by the network. Further, if the UE needs to establish the DTLS session, then necessary credentials are required in the UE to perform the server authentication.

On the technical aspects, How the UE knows whether to use normal DNS request or DNS over DTLS?

[Huawei] My concern is that why does the SMF need to provide the DNS related security information to UE, e.g. credentials, certificate.

It should be left to UE’s implementation or reconfiguration. That’s much more reasonable.

[Samsung] The SMF provides the configuration for the PDU session (QoS rule, IP address for the UE, Security policy, like so), so SMF needs to provide the DNS related security information also to the UE based on the selected DNS Server IP address (for example, SMF may consider not to use DNS over DTLS, if the user plane security policy is enabled for a PDU session and provide a DNS server IP address appropriately). How the UE implementation can handle it, it is not possible when considering further the roaming scenarios?

Our concern is UE may go out of service, if network does not provide proper indication and configuration.

As WID and LS are dependent on these contributions, would like to go with r3 and if any changes required can be addressed in the next meeting. As r2 is not a complete solution, it is not acceptable to include new features in the next meeting to address it.

[Huawei] I’m fine with S3-201392 (was S3-201275) if it can be corrected as below:

“Clause X (Informative)

Security measures specified in Annex X of TS 33.501 [43], can be used to protect the DNS and ICMP messages that are carried over the user plane.” We think this is clear enough. However, I’m wondering whether we can refer to Informative annex in the normative text of TS 33.401.

I am not sure adding a new clause is appropriate here.

It may be cleaner to just add a new informative Annex (Y) to TS 33.401 that refers to the new Annex (X) in TS 33.501. This will also allow us to make any changes or corrections in the future to EPS only if needed. I have uploaded r1 to the drafts folder implementing this approach.

Please have a look.

I will clean up the cover page and removal of 5.1.4 text in the final version.

[Huawei] I’m fine with r1

**Blockers:**

**Expected Status after email approval (unless further comments): Approved**

|  |  |  |
| --- | --- | --- |
| S3‑201295 | Protection of DNS messages  | Samsung |

[Secretary]

* WID code is TEI16, not TEI-16.
* Clause 2 is missing from the clauses affected.
* The NOTE is normative, since it is introducing recommendations. Just remove the NOTE and make it plain text.

[Huawei] As I expressed yesterday, since this solution has impact on EPC, we don’t want any impact on EPC in R16. On the other hand, Qualcomm’s solution does not affect EPC, and it’s agreed to be as an Informative Annex. So I can’t agree this proposal now.

[Samsung] With out indication from the network (EPC), how the UE knows whether to use normal DNS or DNS over DTLS for the EPC provided DNS IP address?

**Blockers: Huawei**

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

|  |  |  |
| --- | --- | --- |
| S3‑201296 | UP integrity protection for UP Signalling messages  | Samsung |

[DT] **Summary:** This document should be noted.

**Motivation:**

> To separate and protect sensitive traffic (like DNS, ICMP) in a dedicated PDU sessions that support UP IP, for 5GS. (Solution #1, TR 33.853)

-> We think this won’t be a quick solution because today's networks and UEs are not designed to perform this separation. Althrough, this proposal seems to target 5GC-capable UEs and networks it is not clear how this would work. Policy-based routing both on UE and network side, depending on the traffic type? Existing IP stacks don't support sending ICMP related to IP address A via IP address B. This separation might work for DNS (in theory) but also in UE and network practice?

This needs more feedback from UE and network vendors as well as from RAN2, SA2, CT1.

[NCSC] I agree with Thomas, and would also add that picking out specific types of traffic to integrity protect is messy, and leaves room for it to be done wrong. From a crypt point of view, mandating UPIP is cleaner, and has the benefit of preventing any similar attacks.

[Samsung] I uploaded a discussion paper ([S3-201329](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_99e/Docs/S3-201329.zip)) for information on how the proposal in S3-201296 works.

I request clarification on DTAG and NCSC comments:

@Thomas,

1. Would like to know little more details on "We think this won’t be a quick solution because today's networks and UEs are not designed to perform this separation" ?. Currently 5GS supports multiple slices, multiple DNNs within a slice and supporting multiple QoS flows within a DNN. Also 5GS supports sending redundant PDU sessions for URLLC scenarios. Why UEs are not designed to perform this separation?

2. Regarding your comment "how this would work.", I uploaded a new doc (S3-201329: <https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_99e/Docs/S3-201329.zip>) for provide illustrative flow on how this proposal works.

3. If we need feedback from other working groups then this CR can be conditionally agreed in SA3 and other WGs can send their feedback to SA plenary directly before approval (which is inline with SA task to SA3).

@James  "mandating UPIP is cleaner", means you mean mandating both "support" and "usage"?

[NCSC] I believe this argument came up last meeting quite a lot, so I can repeat some of the responses that were raised there, which still hold.

As Mauro said: 3GPP has supported the possibility for a MNO to use, or not use, encryption since forever and this possibility has never been a valid argument to say that there is no reason to support encryption. So this type of argument does not hold. The MNO needs to be put in a position to decide if a certain service requires - or does not require – UPIP, and if UPIP is deemed as needed then it shall work without any rate restriction.

As Marcus said: using or not using UPIP should be based on the operator’s network policy

As Tim said: there are at least 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.

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).

[Telecom Italia] I would like **to confirm** that *3GPP has supported the possibility for a MNO to use, or not use, encryption since ever and this possibility has never been a valid argument to say that there is no reason to support encryption. So this type of argument does not hold. The MNO needs to be put in a position to decide if a certain service requires - or does not require – UPIP, and if UPIP is deemed as needed then it shall work without any rate restriction.*

Shortly, “*being optional for use*” cannot be interpreted as “*it does not worth to support it, we can live without it*”...

[Samsung (to NCSC Comment)] Then I do not agree with the comment “mandating UPIP is cleaner”, as it indicates mandatory to support and optional to use. If UP IP is disabled for a service by the serving network (whatsoever reason, even if the UE and the gNB support full rate UPIP), then GSMA referenced attacks are not addressed by SA3.

[Futurewei] I agree with the view that mandating UPIP is cleaner. Operators manage their security policy based on various factors.   With UE and the network fully support UPIP, it gives the operator tools and means to manage their security policy effectively, whatever that security policy is.

Solutions that deal with only a specific type of traffic may work in the short run but they should be considered as patch-work at best. If vulnerabilities are found on other type of traffic, what do you do?  Do you keep on adding other type of traffic to integrity protect?  At some point, you may end up adding more and more type of traffic to integrity protect it becomes a nightmare to manage.  It is therefore cleaner to mandate UPIP period.

[Samsung] It is cleaner to mandate UPIP, but this heavy requirement is too late for Rel-16.

This proposal is not an alternative for “mandating UPIP”. This proposal is a means to manage serving network security policy effectively when UPIP is not used.

As detailed in S3-201329, it shall be possible to add other type of traffic to integrity protection (as it is under the control of the operator), if the operator want to protect some traffic  (due to potential vulnerabilities) and other traffic without protection (for performance).

When support for UP IP data rates increases in the upcoming releases, establishment of dedicated PDU sessions will reduce.

If managing the security policy based on various factors is not nightmare, why addition of the more type of traffic becomes a nightmare to manage.

[Futurewei] I don’t agree that 1) mandating UPIP is heavy requirement and 2) it’s too late for R16.  Operators have vast experience managing their network security policies but waiting to see if another type of traffic becomes vulnerable due to the lack of UPIP should make every operator very nervous. No?  Just ask any operator.

[Interdigital] I agree that it might be useful to hear operators’ opinions here.

[Qualcomm] I don’t think comparing encryption and integrity protection here is entirely valid wrt mandating support vs use. The former has to be optional to use  due to regulatory requirements as use of encryption is forbidden in certain cases (reason why for control plane in 4G/5G, we make use of integrity protection mandatory but not the use of encryption). OTOH, there is no such restriction wrt integrity protection (reason why its use is mandatory for control plane).

If you want to rely on UP IP to mitigate the attacks described in the GSMA LS, then the only option is to mandate the use of UP IP as well just like for control plane. If use of UP IP cannot be mandated, then we need to look for alternative mitigations if you are really concerned about these threats.

[Vodafone] If these solutions are introduced, is your position that SA3 should not then mandate full rate UPIP in any future release (because it won’t be needed)? Or is it rather that full rate UPIP can and should be introduced, but not as early as R16, because (as Samsung argue in S3-201297) more time is needed to study the implications? Or something else?

Just trying to understand the big picture – it maybe that the dedicated solution approach and the full rate UPIP approach are not mutually exclusive.

[Samsung] If these solutions are introduced, is your position that SA3 should not then mandate full rate UPIP in any future release (because it won’t be needed)?

Rajvel> Particularly this solution (S3-201296) does not prevent mandating full rate UPIP in any future releases. In fact, this solution apply UP IP on certain or all data traffic based on network configuration. If the network configures UP IP for a particular application/DNN, then dedicated PDU session is not needed for that application.

Or is it rather that full rate UPIP can and should be introduced, but not as early as R16, because (as Samsung argue in S3-201297) more time is needed to study the implications?

 Rajvel> Yes, full rate UPIP can and should be introduced, but not as early as R16.

Or something else? Just trying to understand the big picture – it maybe that the dedicated solution approach and the full rate UPIP approach are not mutually exclusive.

 Rajvel> Dedicated solution approach (if serving network want to protect only certain type of traffic) and the full rate UPIP approach (if serving network want to enable UP IP for all traffic) can exist together and will complement each other.

[DT] Thank you for providing the detailed description of your intended solution. I understand your intention to protect DNS because that's used by the aLTEr attack plus ICMP because that is used by the IMP4GT attack as an reactive approach.

Am I right assuming:

1. that this protection would be based on a feature which is **optional** i.e. **URSP** ?
Do you propose then to make URSP mandatory?
DT does **not** see UE local configuration as an option for operators.
2. we need at least 2 bearers:

• “slow speed” UPIP’ed for the DNS requests

• “high speed” for the mobile broadband

How does the interaction work ? What are the implications on resource management ? What are the implications on delay ? … I still assume that this would require a full study in SA2 and RAN2 for those aspects …

[Samsung response (in Brown)]

1. that this protection would be based on a feature which is **optional** i.e. **URSP** ?
Do you propose then to make URSP mandatory?
DT does **not** see UE local configuration as an option for operators.

 => To my understanding URSP is not a optional feature it is mandatory feature,

TS 23.501 :

#### 5.15.5.3 Establishing a PDU Session in a Network Slice

--snip---

The UE shall store and use the URSP rules, including the NSSP, as described in TS 23.503 [45]. When a UE application associated with a specific S-NSSAI requests data transmission:

and TS 23.503:

### 4.2.2 UE policy control requirements

The 5GC shall be able to provide policy information from the PCF to the UE. Such policy information includes:

- Access Network Discovery & Selection Policy (ANDSP): It is used by the UE for selecting non-3GPP accesses network.

- UE Route Selection Policy (URSP): This policy is used by the UE to determine how to route outgoing traffic. Traffic can be routed to an established PDU Session, can be offloaded to non-3GPP access outside a PDU Session, or can trigger the establishment of a new PDU Session.

- V2X Policy (V2XP): This policy provides configuration parameters to the UE for V2X communication over PC5 reference point or over PC5 reference point or both. V2X Policies are defined in TS 23.287 [28].

 ---snip-----

 Clause (6.1.2.2)

The ANDSP and URSP shall be provided from the PCF to the AMF via N15/Namf interface and then from AMF to the UE via the N1 interface as described in TS 23.502 [3] clause 4.2.4.3. The AMF shall not change the ANDSP and the URSP provided by PCF.

1. we need at least 2 bearers:

• “slow speed” UPIP’ed for the DNS requests

• “high speed” for the mobile broadband

How does the interaction work ? What are the implications on resource management ? What are the implications on delay ? …

 => To address your concerns, the two bearer can have same QoS policy.

I still assume that this would require a full study in SA2 and RAN2 for those aspects …

=>  Yes, SA3 can send an LS to SA2 and RAN2 (may be, as there is no impact to the RAN procedures).

[Huawei] There are several threads of this topic.. I just remind the progress of other group. For the following suggestions, I don’t think it’s suitable at this point. SA2 and RAN2 R16 is frozen already, which means it’s too late for them to visiting this specific issue, i.e. specific QoS or DNN. Hence, we need a simple way to address this issue obviously.

[Samsung] @Alf, thank you for the comments.

    - I revised the CR in draft-S3-201296-r1 to include appropriate network elements and procedures. Hope it address you concern.

    - Regarding ROHC in terms of redirection, in my analysis, ROHC are not applied to the DNS packets. The attack on DNS is possible, because the DNS packet goes alone (without concatenation or segmentation at RLC) as it is first packet in a PDU session. But for other packets, malleability attack is not possible as the RLC performs concatenation and/or segmentation, so it is difficult to mount known-plain text attack.

 @Rong, thank you the comments.

    - Specific QoS for DNN is operational configuration and does not need any change in the SA2/RAN2 specifications

    - S3-201296 does not require any change and discussion is to check the solution feasibility, Even if any identified, as per SA guideline (task to SA3 from SA March'2020) SA3 can request SA2 to consider.

 @All, please consider the revised the CR in draft-S3-201296-r1, which includes appropriate network elements and procedures.

[DT] Thank you for this revision. I still do believe that integrity protecting of only specific types of traffic will not be as effective as protecting all, but for the sake of making any progress, please remove the blocking statement of DT (that was captured in <SA3#99e - UPIP Rapporteurs Minutes Day2.docx>.

[Samsung] Thanks a lot for withdrawing the objection. I really appreciate it.

[secretary]

* It should be TEI16 on the cover page, not TEI-16, BUT…
* …I suggest to include this CR as part of the normative WID in tdoc S3-201308, on UP IP stuff. So you put UP\_IP SEC on the cover page and Noame should note this as submitted to SA together with the WID.

[DoCoMo] responding to the latest message on 296, because I don’t really know which thread is the “correct” one…

Which part of what is described now is really new behaviour (i.e. requiring mandatory text and changes to the existing system, rather than reconfiguration of the operator network).

I also don’t understand how the UE will be configured. Is this part of the existing 3GPP spec that the operator can configure a UE to use two DNNs?

How does all of this work in roaming scenarios?

And regarding my comment on ROHC. I was not trying to imply DNS using ROHC. But all applications that use ROHC can be vulnerable to redirection attacks without UPIP. It has long been accepted in the research community that encryption without integrity protection doesn’t work against active attackers.

[Samsung] I uploaded a discussion paper ([S3-201329](https://protect2.fireeye.com/url?k=1642a86a-4b8e61ee-16432325-0cc47aa8f5ba-8474f55c03b3652b&q=1&u=https%3A%2F%2Fnam11.safelinks.protection.outlook.com%2F%3Furl%3Dhttps%253A%252F%252Fprotect2.fireeye.com%252Furl%253Fk%253D64ed033d-392302ee-64ec8872-000babff317b-9cf57aa233935c8d%2526q%253D1%2526u%253Dhttps%25253A%25252F%25252Fnam11.safelinks.protection.outlook.com%25252F%25253Furl%25253Dhttps%2525253A%2525252F%2525252Fprotect2.fireeye.com%2525252Furl%2525253Fk%2525253D8cf041b9-d13e400d-8cf1caf6-000babdfecba-fb5b1792b4a8e057%25252526q%2525253D1%25252526u%2525253Dhttps%252525253A%252525252F%252525252Feur03.safelinks.protection.outlook.com%252525252F%252525253Furl%252525253Dhttps%25252525253A%25252525252F%25252525252Fwww.3gpp.org%25252525252Fftp%25252525252FTSG_SA%25252525252FWG3_Security%25252525252FTSGS3_99e%25252525252FDocs%25252525252FS3-201329.zip%2525252526data%252525253D02%25252525257C01%25252525257Cjames.o%252525252540NCSC.GOV.UK%25252525257Cec017024b6154b05571708d7f5aa5485%25252525257C14aa5744ece1474ea2d734f46dda64a1%25252525257C0%25252525257C0%25252525257C637247984220329763%2525252526sdata%252525253DcjjpxivMET5SJhqOoikRwh1R%25252525252BzaqV6rpg31jJSTPNDo%25252525253D%2525252526reserved%252525253D0%252526data%25253D02%2525257C01%2525257Cmwong%25252540FUTUREWEI.COM%2525257Cdad4e245b5e24d03b4a708d7f5c85a60%2525257C0fee8ff2a3b240189c753a1d5591fedc%2525257C1%2525257C0%2525257C637248113173392781%252526sdata%25253DwugJtpKOnfJVz35o4P4IOYfI9Tpc0z4Gscf1dVFR304%2525253D%252526reserved%25253D0%26data%3D02%257C01%257Cmwong%2540FUTUREWEI.COM%257Cca69ad3d1ebe4cea938a08d7f5df1365%257C0fee8ff2a3b240189c753a1d5591fedc%257C1%257C0%257C637248210773566104%26sdata%3DHBx2O%252BAGcHV9Cf1GJcBkbcA4uhWyt8Uau2WpkXz68iU%253D%26reserved%3D0)) for information on how the proposal in S3-201296 works. All your question are answered in the discussion paper. It is reconfiguration of the operator network and does not changes to the existing system.

Even though it is answered in the [S3-201329](https://protect2.fireeye.com/url?k=1642a86a-4b8e61ee-16432325-0cc47aa8f5ba-8474f55c03b3652b&q=1&u=https%3A%2F%2Fnam11.safelinks.protection.outlook.com%2F%3Furl%3Dhttps%253A%252F%252Fprotect2.fireeye.com%252Furl%253Fk%253D64ed033d-392302ee-64ec8872-000babff317b-9cf57aa233935c8d%2526q%253D1%2526u%253Dhttps%25253A%25252F%25252Fnam11.safelinks.protection.outlook.com%25252F%25253Furl%25253Dhttps%2525253A%2525252F%2525252Fprotect2.fireeye.com%2525252Furl%2525253Fk%2525253D8cf041b9-d13e400d-8cf1caf6-000babdfecba-fb5b1792b4a8e057%25252526q%2525253D1%25252526u%2525253Dhttps%252525253A%252525252F%252525252Feur03.safelinks.protection.outlook.com%252525252F%252525253Furl%252525253Dhttps%25252525253A%25252525252F%25252525252Fwww.3gpp.org%25252525252Fftp%25252525252FTSG_SA%25252525252FWG3_Security%25252525252FTSGS3_99e%25252525252FDocs%25252525252FS3-201329.zip%2525252526data%252525253D02%25252525257C01%25252525257Cjames.o%252525252540NCSC.GOV.UK%25252525257Cec017024b6154b05571708d7f5aa5485%25252525257C14aa5744ece1474ea2d734f46dda64a1%25252525257C0%25252525257C0%25252525257C637247984220329763%2525252526sdata%252525253DcjjpxivMET5SJhqOoikRwh1R%25252525252BzaqV6rpg31jJSTPNDo%25252525253D%2525252526reserved%252525253D0%252526data%25253D02%2525257C01%2525257Cmwong%25252540FUTUREWEI.COM%2525257Cdad4e245b5e24d03b4a708d7f5c85a60%2525257C0fee8ff2a3b240189c753a1d5591fedc%2525257C1%2525257C0%2525257C637248113173392781%252526sdata%25253DwugJtpKOnfJVz35o4P4IOYfI9Tpc0z4Gscf1dVFR304%2525253D%252526reserved%25253D0%26data%3D02%257C01%257Cmwong%2540FUTUREWEI.COM%257Cca69ad3d1ebe4cea938a08d7f5df1365%257C0fee8ff2a3b240189c753a1d5591fedc%257C1%257C0%257C637248210773566104%26sdata%3DHBx2O%252BAGcHV9Cf1GJcBkbcA4uhWyt8Uau2WpkXz68iU%253D%26reserved%3D0), for quick reference:

    - An application can use two PDU sessions and IP descriptors (like, source IP address, port, protocol ID) are used to differentiate the PDU sessions, for example on how application can manage two PDU sessions is detailed for Redundant transmission for high reliability communication in TS 23.501[1] *(clause 5.33.2.1 (Dual Connectivity based end to end Redundant User Plane Paths)).*

   - In roaming scenarios, URSP rules are provided by VPCF via AMF, it is detailed in TS 23.501 and TS 23.503, all references are provided in [S3-201329](https://protect2.fireeye.com/url?k=1642a86a-4b8e61ee-16432325-0cc47aa8f5ba-8474f55c03b3652b&q=1&u=https%3A%2F%2Fnam11.safelinks.protection.outlook.com%2F%3Furl%3Dhttps%253A%252F%252Fprotect2.fireeye.com%252Furl%253Fk%253D64ed033d-392302ee-64ec8872-000babff317b-9cf57aa233935c8d%2526q%253D1%2526u%253Dhttps%25253A%25252F%25252Fnam11.safelinks.protection.outlook.com%25252F%25253Furl%25253Dhttps%2525253A%2525252F%2525252Fprotect2.fireeye.com%2525252Furl%2525253Fk%2525253D8cf041b9-d13e400d-8cf1caf6-000babdfecba-fb5b1792b4a8e057%25252526q%2525253D1%25252526u%2525253Dhttps%252525253A%252525252F%252525252Feur03.safelinks.protection.outlook.com%252525252F%252525253Furl%252525253Dhttps%25252525253A%25252525252F%25252525252Fwww.3gpp.org%25252525252Fftp%25252525252FTSG_SA%25252525252FWG3_Security%25252525252FTSGS3_99e%25252525252FDocs%25252525252FS3-201329.zip%2525252526data%252525253D02%25252525257C01%25252525257Cjames.o%252525252540NCSC.GOV.UK%25252525257Cec017024b6154b05571708d7f5aa5485%25252525257C14aa5744ece1474ea2d734f46dda64a1%25252525257C0%25252525257C0%25252525257C637247984220329763%2525252526sdata%252525253DcjjpxivMET5SJhqOoikRwh1R%25252525252BzaqV6rpg31jJSTPNDo%25252525253D%2525252526reserved%252525253D0%252526data%25253D02%2525257C01%2525257Cmwong%25252540FUTUREWEI.COM%2525257Cdad4e245b5e24d03b4a708d7f5c85a60%2525257C0fee8ff2a3b240189c753a1d5591fedc%2525257C1%2525257C0%2525257C637248113173392781%252526sdata%25253DwugJtpKOnfJVz35o4P4IOYfI9Tpc0z4Gscf1dVFR304%2525253D%252526reserved%25253D0%26data%3D02%257C01%257Cmwong%2540FUTUREWEI.COM%257Cca69ad3d1ebe4cea938a08d7f5df1365%257C0fee8ff2a3b240189c753a1d5591fedc%257C1%257C0%257C637248210773566104%26sdata%3DHBx2O%252BAGcHV9Cf1GJcBkbcA4uhWyt8Uau2WpkXz68iU%253D%26reserved%3D0).

[Nokia] Difficult to catch up with all the discussions, we certainly think #296 is a viable solution.

[Huawei] After checking with our SA2 colleagues, we find this solution has huge impact:

Firstly, we should know how current DNS inquiry procedure works, i.e. the SMF will allocate DNS IP and UE IP for each PDU session. Let’s assumes that there are two PDU sessions:

PDU session 1: UE IP 1, DNS IP 1, DNN1 (the related UPF is located in Beijing)

PDU session 2: UE IP 2, DNS IP 2, DNN2 (the related UPF is located in New York)

When the user wants to use APP1 (binding to PDU session 1), the ME will inquiry APP1’s IP using UE IP1 and DNS IP1, the DNS server will allocate a nearby APP server (e.g. Beijing server) according to UE IP1 (The UE IP1 shows that the related UPF is located in Beijing)

When the user wants to use APP2 (binding to PDU session 2), the ME will inquiry APP2’s IP using UE IP2 and DNS IP2, the DNS server will allocate a nearby APP server (e.g. New York server) according to UE IP2 (The UE IP2 shows that the related UPF is located in New York).

Now, we go through this solution.

A URSP is sent to the UE (if the UE wants to do DNS inquiry, the UE shall establish a new PDU session to DNN3)

Now, there will be a new PDU session 3: UE IP 3, DNS IP 3, DNN3 (the related UPF may be located in Shanghai)

When the user wants to use APP2 (binding to PDU session 2), since the ME already establish a PDU session 3 for DNS inquiry, the ME will inquiry APP2’s IP using UE IP3 and DNS IP3, the DNS server will allocate a nearby APP server (e.g. Shanghai server) according to UE IP3 (The UE IP3 shows that the related UPF is located in Shanghai). However, the server should be located in New York. We are not sure whether the UE could access this APP server via New York’s UPF.

Thus, the solution has the following problems:

1. The solution obeys existing DNS inquiry logic, and may make UE unavailable for service:

Since DNS server could allocate a nearby server IP according to source IP, but the source IP is bind to specific PDU session, newly established PDU session obeys this principle, and may get wrong server IP.

1. The solution has UE impact:

How does the PDU session 2 gets server’s IP from PDU session 3? There is no interaction between two PDU sessions for now.

1. The solution introduces big configuration complex

Operators need to allocate a specific DNN to all of DNS servers, which is not flexible.

Thus, it is proposed to NOTE this contribution this time.

[Ericsson] Ericsson propose to note the contribution.

Not sure if we have understood the proposal correctly. We have some initial questions regarding this proposal:

* Generic UE configuration update procedure is used for parameters and information under control of the AMF. URSP is not access and mobility related information but session related information. In this case information between PCF and UE. Such information shall be transparent to the AMF and for this the NAS transport procedure is used.

* The proposal will double the number of PDU Sessions.

* It is proposed that DNS and ICMP are sent on separate PDU Session. But in general ICMP is tied to the link, i.e. it needs to be sent separately on each link / PDU Session. Some ICMP messages may be possible to direct to another link, but the main ones used in 5G (e.g. RS, RA) cannot be sent on the other PDU Session so the solution will not work for those.

* For DNS the two PDU Sessions need to be equivalent, otherwise the DNS reply from one PDU Session will not be applicable for application traffic sent on the other PDU Session. How can that be ensured? The two PDU Sessions may be served by different SMFs and different UPFs on different data centers.

* The UE would need to know which PDU Sessions are “paired up”. For example, if the UE has the following PDU Sessions:
	+ PDU Session 1 to DNN1: application traffic to internet (without UP IP)
	+ PDU Session 2 to DNN2: DNS, ICMP (with UP IP)
	+ PDU Session 3 to DNN3: IMS
	+ PDU Session 4 to DNN4: Corporate network

In this case the UE can use PDU Session 2 for DNS/ICMP only for one DNN (say Internet DNN1). Sending DNS request for IMS or the corporate network on PDU Session 2 will not work. How will UE know that PDU Session 2 DNS, ICMP is just for the applications on PDU Session 1?

We are not sure if URSP can solve that? Would updates be needed so that URSP can link together DNN1 and DNN2 in some way?

[Samsung] On your assumption: Now, there will be a new PDU session 3: UE IP 3, DNS IP 3, DNN3 (the related UPF may be located in Shanghai)

-Rajvel> If the network assigns UE IP 3 (belong to same DNN1) and same DNS IP1 it will work. Why network assigns some other DNS IP 3 for the same application ID with matching traffic descriptor.

 @Monica,

I uploaded a discussion paper ([S3-201329](https://protect2.fireeye.com/url?k=1642a86a-4b8e61ee-16432325-0cc47aa8f5ba-8474f55c03b3652b&q=1&u=https%3A%2F%2Fnam11.safelinks.protection.outlook.com%2F%3Furl%3Dhttps%253A%252F%252Fprotect2.fireeye.com%252Furl%253Fk%253D64ed033d-392302ee-64ec8872-000babff317b-9cf57aa233935c8d%2526q%253D1%2526u%253Dhttps%25253A%25252F%25252Fnam11.safelinks.protection.outlook.com%25252F%25253Furl%25253Dhttps%2525253A%2525252F%2525252Fprotect2.fireeye.com%2525252Furl%2525253Fk%2525253D8cf041b9-d13e400d-8cf1caf6-000babdfecba-fb5b1792b4a8e057%25252526q%2525253D1%25252526u%2525253Dhttps%252525253A%252525252F%252525252Feur03.safelinks.protection.outlook.com%252525252F%252525253Furl%252525253Dhttps%25252525253A%25252525252F%25252525252Fwww.3gpp.org%25252525252Fftp%25252525252FTSG_SA%25252525252FWG3_Security%25252525252FTSGS3_99e%25252525252FDocs%25252525252FS3-201329.zip%2525252526data%252525253D02%25252525257C01%25252525257Cjames.o%252525252540NCSC.GOV.UK%25252525257Cec017024b6154b05571708d7f5aa5485%25252525257C14aa5744ece1474ea2d734f46dda64a1%25252525257C0%25252525257C0%25252525257C637247984220329763%2525252526sdata%252525253DcjjpxivMET5SJhqOoikRwh1R%25252525252BzaqV6rpg31jJSTPNDo%25252525253D%2525252526reserved%252525253D0%252526data%25253D02%2525257C01%2525257Cmwong%25252540FUTUREWEI.COM%2525257Cdad4e245b5e24d03b4a708d7f5c85a60%2525257C0fee8ff2a3b240189c753a1d5591fedc%2525257C1%2525257C0%2525257C637248113173392781%252526sdata%25253DwugJtpKOnfJVz35o4P4IOYfI9Tpc0z4Gscf1dVFR304%2525253D%252526reserved%25253D0%26data%3D02%257C01%257Cmwong%2540FUTUREWEI.COM%257Cca69ad3d1ebe4cea938a08d7f5df1365%257C0fee8ff2a3b240189c753a1d5591fedc%257C1%257C0%257C637248210773566104%26sdata%3DHBx2O%252BAGcHV9Cf1GJcBkbcA4uhWyt8Uau2WpkXz68iU%253D%26reserved%3D0)) for information on how the proposal in S3-201296 works. Please checks it answers all your questions.

Please see my inline response.

* Generic UE configuration update procedure is used for parameters and information under control of the AMF. URSP is not access and mobility related information but session related information. In this case information between PCF and UE. Such information shall be transparent to the AMF and for this the NAS transport procedure is used.

                - Rajvel> Please check TS 23.501 and TS 23.503, reference are provided in [S3-201329](https://protect2.fireeye.com/url?k=1642a86a-4b8e61ee-16432325-0cc47aa8f5ba-8474f55c03b3652b&q=1&u=https%3A%2F%2Fnam11.safelinks.protection.outlook.com%2F%3Furl%3Dhttps%253A%252F%252Fprotect2.fireeye.com%252Furl%253Fk%253D64ed033d-392302ee-64ec8872-000babff317b-9cf57aa233935c8d%2526q%253D1%2526u%253Dhttps%25253A%25252F%25252Fnam11.safelinks.protection.outlook.com%25252F%25253Furl%25253Dhttps%2525253A%2525252F%2525252Fprotect2.fireeye.com%2525252Furl%2525253Fk%2525253D8cf041b9-d13e400d-8cf1caf6-000babdfecba-fb5b1792b4a8e057%25252526q%2525253D1%25252526u%2525253Dhttps%252525253A%252525252F%252525252Feur03.safelinks.protection.outlook.com%252525252F%252525253Furl%252525253Dhttps%25252525253A%25252525252F%25252525252Fwww.3gpp.org%25252525252Fftp%25252525252FTSG_SA%25252525252FWG3_Security%25252525252FTSGS3_99e%25252525252FDocs%25252525252FS3-201329.zip%2525252526data%252525253D02%25252525257C01%25252525257Cjames.o%252525252540NCSC.GOV.UK%25252525257Cec017024b6154b05571708d7f5aa5485%25252525257C14aa5744ece1474ea2d734f46dda64a1%25252525257C0%25252525257C0%25252525257C637247984220329763%2525252526sdata%252525253DcjjpxivMET5SJhqOoikRwh1R%25252525252BzaqV6rpg31jJSTPNDo%25252525253D%2525252526reserved%252525253D0%252526data%25253D02%2525257C01%2525257Cmwong%25252540FUTUREWEI.COM%2525257Cdad4e245b5e24d03b4a708d7f5c85a60%2525257C0fee8ff2a3b240189c753a1d5591fedc%2525257C1%2525257C0%2525257C637248113173392781%252526sdata%25253DwugJtpKOnfJVz35o4P4IOYfI9Tpc0z4Gscf1dVFR304%2525253D%252526reserved%25253D0%26data%3D02%257C01%257Cmwong%2540FUTUREWEI.COM%257Cca69ad3d1ebe4cea938a08d7f5df1365%257C0fee8ff2a3b240189c753a1d5591fedc%257C1%257C0%257C637248210773566104%26sdata%3DHBx2O%252BAGcHV9Cf1GJcBkbcA4uhWyt8Uau2WpkXz68iU%253D%26reserved%3D0).

* The proposal will double the number of PDU Sessions.

                 - Rajvel> Yes only for the PDU sessions which does not support UPIP

* It is proposed that DNS and ICMP are sent on separate PDU Session. But in general ICMP is tied to the link, i.e. it needs to be sent separately on each link / PDU Session. Some ICMP messages may be possible to direct to another link, but the main ones used in 5G (e.g. RS, RA) cannot be sent on the other PDU Session so the solution will not work for those.

                    - Rajvel> It is already addressed in TS 23.501. Please check *(TS 23.501 clause 5.33.2.1 (Dual Connectivity based end to end Redundant User Plane Paths)).*

* For DNS the two PDU Sessions need to be equivalent, otherwise the DNS reply from one PDU Session will not be applicable for application traffic sent on the other PDU Session. How can that be ensured? The two PDU Sessions may be served by different SMFs and different UPFs on different data centers.

                         - Rajvel> It is already addressed in TS 23.501. Please check *(TS 23.501 clause 5.33.2.1 (Dual Connectivity based end to end Redundant User Plane Paths)).*

* The UE would need to know which PDU Sessions are “paired up”. For example, if the UE has the following PDU Sessions:
	+ PDU Session 1 to DNN1: application traffic to internet (without UP IP)
	+ PDU Session 2 to DNN2: DNS, ICMP (with UP IP)
	+ PDU Session 3 to DNN3: IMS
	+ Rajvel> PDU Session 5 to DNN3: DNS, ICMP (with UP IP)
	+ PDU Session 4 to DNN4: Corporate network
	+ Rajvel> PDU Session 6 to DNN4: DNS, ICMP (with UP IP)

In this case the UE can use PDU Session 2 for DNS/ICMP only for one DNN (say Internet DNN1). Sending DNS request for IMS or the corporate network on PDU Session 2 will not work. How will UE know that PDU Session 2 DNS, ICMP is just for the applications on PDU Session 1?

  - Rajvel> If the PDU Sessions 3 and 4 are to different DN, then each can create separate PDU Sessions as mentioned above.

We are not sure if URSP can solve that? Would updates be needed so that URSP can link together DNN1 and DNN2 in some way?

- Rajvel>If we need feedback from other working groups then this CR can be conditionally agreed in SA3 and other WGs can send their feedback to SA plenary directly before approval (which is inline with SA task to SA3).

[DT] Some more thoughts on this item. The feature from TS 23.501[1] (*clause 5.33.2.1 (Dual Connectivity based end to end Redundant User Plane Paths*) might be usable as described. But in principle, redundant data paths (=same data transmitted over two paths for reliability) in the TS are different from two distinct paths for different data that we need here.

I would like to get some info on:

* Do 5CG vendors think this is a feasible use case for the feature, and whether their 5GC products support it?
* Moreover, TS 23.501 clause 5.33.2.1 has a long list of "aspects are within the responsibility of the operator and are not subject to 3GPP standardization", amongst them "UEs support dual connectivity". At the moment it is not clear to me how the operator can be responsible for that?

[Huawei] The main concern is that the solution has huge impact on SA2 procedure, e.g. DNS inquiry. I got the feedback from SA2 colleagues, they think this solution has a lot of huge and technical problem and it doesn’t work.

Since we are not architectural experts, I suggestion if we would like to proceed, we have to ask SA2’s view on this. It’s not a simple security solution, just a security requirement. How to establish the specific DNN PDU Session is SA2’s scope.

So currently, I can’t agree this. One way forward is that we can send a LS to SA2 to officially ask whether the solution is workable.

[Ericsson] Ericsson has the same view as Huawei. We would feel more comfortable with asking SA2 by sending a LS to SA2 to ask whether the solution is workable.

**Blockers: Huawei, Ericsson**

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

|  |  |  |
| --- | --- | --- |
| S3‑201297 | Integrity Protection for UP Signalling messages  | Samsung |

**[DT] Summary:** This document should be noted.

**Motivation:**

**On the Proposal #1**: SA3 needs to perform more study on the issues (like failure handling, failure reporting, performance analysis) in collaboration with other WGs to activate UP IP at full data rate in the upcoming releases for maintaining QoS/QoE.

-> We don't see the issue. If the UE tries to send more data than it can it will fail IP and traffic will be discarded. This is a hypothetical issue that will be found by standard device release testing and does not need a specific handling in 3GPP. The same could happen today without UP IP: the UE "tries" to "fill" a radio bearer with data but fails to deliver it at the bearer's data rate.

**On the Proposal #2**: Considering the Rel-16 time limitation and the amount of work required on further study in activating UP IP at full data rate properly, SA3 need to identify interim solutions for Rel-16 on how best the threats (on DNS and ICMP) can be mitigated when UP IP is disabled.

-> Any interim solution would need further study that cannot be completed in the normative phase for Rel-16. **From our view, the operators' proposal to mandate full-rate UP IP is the only option that can be defined in time for Rel-16**

**On the Proposal #3:** Current 64 kbps UPIP capability is too limited. SA3 should decide to have more granularities for UP IP capabilities and should request RAN2/CT1 work on defining more granularity for UPIP data rates for Rel-16.

-> Looks too complex, and completely new negotiation mechanism needed.

**On the Proposal #4:** Interim solutions to mitigate GSMA referenced attack is needed for EPS also.

-> This is part of the ongoing UP IP study. We don't see an "interim" solution for EPS, but a study for normative work in Rel-17

[Samsung]->

To note 1 comment… > Implementation is always based on stable specification. Referencing to the clause 7.3.2 in TS 33.401, which has the following Note.

NOTE: The handling of UP integrity check failures by an RN is an implementation issue. TS 36.323 [12] intentionally does not mandate any action for a failed integrity check (not even sending an indication of failure to higher layers). Consequently, depending on the implementation, the message failing integrity check is, or is not, silently discarded. This is in contrast to the handling of a failed RRC integrity check by a UE, cf. the NOTE in clause 7.4.1 of the present document.

To note 2 comment:

> Provided the details in S3-201329, which uses the existing procedures.

To Note 3 comment:

> Proposal is to have more granularities for UPIP capabilities (for example, say between 256 Kbps and 5 Gbps) instead of only 64Kbps or Full rate.  Its not a new negotiation mechanism

To Note 4 comment:

> Proposal is to address the GSMA referenced attack for LTE-only UEs.

[Futurewei] I do not agree with Proposals 1) 2), and 4) at all.  For Proposal 3) I only agree with the first sentence which is “Current 64 kbps UPIP capability is too limited”

UPIP is one of the distinguishing features of 5G and 3GPP had to live with two years of the 64 kpbs limitation due to device availability. I would not like to have this discussion two years down the road.  As for EPS, if we can fix it without introducing backward compatibility, then we can study how to fix it.

[KPN] Regarding proposal #3:

As far as I understand the situation the network (i.e. the operator) has the option of ‘requiring’ UP IP. And if this is required (by the network) then the UE has to provide UP IP. If it cannot do it at full rate, then currently it has to use 64 kbps.

By adding a larger range of data rates, the UE can do UP IP at a higher rate (even if it does not support it at full rate). This would ‘solve’ the situation of UEs without ‘full data rate UP IP support’.

And I agree with Rajvel, that it is not a negotiation mechanism, but only a richer list of UE capabilities.

[Vodafone] My view on Proposal #3:

* If we can agree to full data rate UPIP support in UEs from R16 – which is what I would prefer – then we don’t need to introduce negotiation of a wider range of supported data rates.
* If not – if we can’t achieve full data rate UPIP support in all devices until a later release – then introducing negotiation of a wider range of supported data rates is helpful.  It allows us to make better use of whatever UPIP support we have.

I guess there’s a reluctance to introduce negotiation of a wider range of supported data rates, because that’s seen as admitting defeat on the full rate UPIP support that I believe most people want.

[DT] on -> reluctance to introduce negotiation of a wider range of supported data rates, because that’s seen as admitting defeat on the full rate UPIP support

Another issue of this negotiation is the added complexity that was already discussed in CT1 and lead to rejection of that idea.

Up to now, 3GPP procedures never had any dependency between data rate and security negotiation. Negotiation of data rate and security are independent.

The Rel-15 "all or nothing (=64 kbps) negotiation" can at least be handled by a suitable network configuration, i.e. grant the UE "all (full speed w/o UP IP) or nothing (64 kbps with UP IP)" depending on operator policy.

But adding further speed steps brings us if-then-else decisions between both procedures (data rate and security negotiation) that might require different message flows and iterations.

I think of aspects like:

- network to enforce UP IP only for UEs supporting a specific minimum data rate with UP IP

- network to allow specific UEs to run high data rate without UP IP depending on what criteria? Subscription profile? Traffic type?

- network needs to "know" in advance whether enforcing UP IP would be acceptable to the UE's owner and the service that will be consumed over the bearer to be set up

- UE may need to ask the user if she prefers speed or security, per application

- UE/user may "change their mind" about the requested bearer data rate when they learn the network will enforce UP IP

- UE needs to steer different traffic types into different bearers at different speed/IP settings

I don't see how more speed steps will provide a quick improvement.

**Blockers: DT, Futurewei**

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

|  |  |  |
| --- | --- | --- |
| S3‑201298 | Conclusion to Key Issue #5  | Samsung |

[Huawei] Huawei proposes to note this contribution, the reason is stated in S3-201296.

**Blockers: None**

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

|  |  |  |
| --- | --- | --- |
| S3‑201305 | pCR to TR 33.853 (UPIP): addition of new solution - use NR PDCP for LTE  | VODAFONE Group Plc |

[Qualcomm] In SA3#98bis-e, the original version of this solution (S3-200631) was discussed and Qualcomm provided some comments on it ( please refer to the email thread: [SA3#98bis-e][2.11,UPIP][S3-200631]pCR to TR 33.853 (UPIP): addition of new solution - used NR PDCP for LTE).

We believe the main idea of this revised solution is same as that of the original version.

With that, we still have the same comments.

In UE, use of NR-PDCP for LTE does not necessarily mean full-rate support of UP IP for LTE even when full rate UP IP is supported for NR. Also, use of LTE-PDCP does not prohibit full-rate support of UP IP, e.g., Rel-10 Relay node supports UP IP with LTE PDCP. It is clear that the support of UP IP not related to the PDCP version but related to UE’s capability (just to be clear, it’s not security capability but capability to support full-rate UP IP).

But, this solution describes how PDCP functionality should be implemented inside the UE (i.e., UE’s implementation choice) instead of how to support UP IP in LTE.

Qualcomm still don’t see why this UE’s implementation choice should be documented in the TR.

[Vodafone] S3-201305 is already revised to accommodate the more detailed comments that Qualcomm sent on the last day of the last SA3 emeeting. It describes how something CAN, in the future, be implemented in the UE. Obviously existing LTE UEs are unlikely to support full rate UP IP over LTE… so it’s reasonable for a TR solution candidate to have some UE impact.

The point of a TR like this one is to gather solution ideas and then to evaluate them However, you are still missing the important, main point of this contribution – which does NOT relate to existing terminals. The key difficultly with getting UPIP into operation is likely to be on the base stations where the use of UPIP might well have an impact on the firmware of deployed eNBs. What this contribution describes is how the network (using a mix of existing standards and work already scheduled in RAN for R17) might be “software” upgraded so that legacy eNBs can control remotely located PDCP hardware (e.g. in a gNB). This ‘remote control’ capability may well remove a major obstacle to LTE UPIP becoming utilised.

Note that EXISTING EN-DC capable gNBs (which do not have LTE-PDCP) allow their NR-PDCP to be controlled by remote eNBs.

So, as I already have revised this document to accommodate the comments you sent last time (and you repeated below) I don’t see that there is any reason to NOT include it in the TR. I inserted some more explanation inline below.

In UE, use of NR-PDCP for LTE does not necessarily mean full-rate support of UP IP for LTE even when full rate UP IP is supported for NR.

[CDP: this solution describes new UEs not legacy ones.]

Also, use of LTE-PDCP does not prohibit full-rate support of UP IP, e.g., Rel-10 Relay node supports UP IP with LTE PDCP. It is clear that the support of UP IP not related to the PDCP version but related to UE’s capability (just to be clear, it’s not security capability but capability to support full-rate UP IP).

[CDP: so what? You are free to propose a different solution.]

But, this solution describes how PDCP functionality should be implemented inside the UE (i.e., UE’s implementation choice) instead of how to support UP IP in LTE. [CDP: NO it does not say “should” it says “can”. You are ignoring the network side where EN-DC operators already have NR PDCP deployed remotely from legacy eNBs.]

Qualcomm still don’t see why this UE’s implementation choice should be documented in the TR. [CDP: because it offers better network rollout possibilities.]

[Qualcomm] Thanks for the reply to my comments. Now, I seem to have better understanding of the proposed solution based on the inline comments below.

If I understand correctly, Vodafone is proposing a solution that achieves UP IP over LTE using NR UP IP capability.

If that interpretation is correct, I guess our misunderstanding came from the use of terminology (and perhaps interpretation of the solution from UE’s pov).

As Anand indicated in previous meeting, we assume UP IP is a RAT dependent capability (i.e., LTE UP IP and NR UP IP capabilities), but your solution seems to introduce a new UP IP capability, which has never been discussed during the study.

Then, a question is how such capability would be signaled. I believe UE should be able to signal a new UP IP capability (e.g., UP IP using NR PDCP over LTE) to the network in addition to UP IP over LTE and UP IP over NR.

Also, which algorithm should be used in such case? Should it be LTE algorithm or NR algorithm? I guess which algorithm to use has to be signaled as well. Note that SA3 defined different algorithm code points for LTE and NR, but to support the proposed solution, NR algorithm may be selected for LTE?

Assuming my understanding is correct and you agree with the above, **I am happy to accept your solution for inclusion in the TR with the following Editor’s Notes and some clarifying text**:

EN: how to signal the proposed UP IP capability is FFS

EN: which security algorithms should be selected/signaled for the proposed solution needs to be clarified

Can you please add some clarification text that captures the following aspects (I don’t have good wording and a right place to put it at this point):

* **this solution proposes a mechanism that achieves UP IP over LTE using the NR UP IP capability**
* **the proposed solution is different from (or independent of) LTE UP IP capability**

Would this be acceptable to you?

[Vodafone] Thanks for the reply. I’ve uploaded a “r1” with the updates highlighted in yellow. Hopefully it is acceptable to you.

With regard to your comments on signalling and algorithm choice, I have not checked the details, but (from memory) I suspect that the Rel 10 LTE UP IP added for Relay nodes is also missing the NAS and S1AP signalling that would be needed to control it in a smartphone. (But this check is some work that we should do in the future)

[Qualcomm] R1 looks okay to me. Thanks for the revision and having accepted our comments.

**Blockers:**

**Status at end of meeting (unless there are further comments): Approved (rev 1)**

|  |  |  |
| --- | --- | --- |
| S3‑201307 | LS to RAN2 and CT1 on Updated User Plane Integrity Protection advice  | VODAFONE Group Plc |

[Telecom Italia]Telecom Italia believe that the wording “*from as soon as practical*” currently used in bullets 1-4 is too vague and would end up in making the LS useless, in practice.

Therefore, we would like to propose the following changes ( highlighted in yellow)

1.            *UPIP shall be supported by the UE and the gNB for all NR bearers configured in NR SA (Option 2) regardless of the data rate from Rel-16 onwards.*

*2.            UPIP shall be supported by the UE and the (ng-)eNB for all LTE bearers configured in EN-DC (Option 3 family), LTE/EPC (Option 1) and LTE/5GC (Option 5) regardless of the data rate from Rel-17 onwards.*

*3.            UPIP shall be supported by the UE and the en-gNB for all NR bearers configured in EN-DC (Option 3 family) regardless of the data rate from Rel-17 onwards.*

*4.            UPIP shall be supported by the UE and the ng-eNB/gNB for all LTE/NR bearers configured in NGEN-DC (Option 7 family), NE-DC (Option 4 family) and NR-DC regardless of the data rate from Rel-17 onwards.*

[DT] It is unclear for me why the “S3-201307 - Draft LS Out to RAN2 and CT1 on Updated User Plane Integrity Protection advice”, is stating:

 SA3 advises that it has changed its advice on UPIP to:

1.           UPIP should be supported by the UE and the gNB for all NR bearers configured in NR SA (Option 2) regardless of the data rate from as soon as practical.

2.           UPIP shall be supported by the UE and the (ng-)eNB for all LTE bearers configured in EN-DC (Option 3 family), LTE/EPC (Option 1) and LTE/5GC (Option 5) regardless of the data rate from as soon as practical.

3.           UPIP shall be supported by the UE and the en-gNB for all NR bearers configured in EN-DC (Option 3 family) regardless of the data rate from as soon as practical.

4.           UPIP shall be supported by the UE and the ng-eNB/gNB for all LTE/NR bearers configured in NGEN-DC (Option 7 family), NE-DC (Option 4 family) and NR-DC regardless of the data rate from as soon as practical.

5.           It is recommended that UPIP is always enabled where it can be, although it is recognised that legacy equipment will need to be catered for.

Why is in case of Option 2 a “should” while all others have a “shall” ?  Actually DTAG would like to see the “shall” everywhere…but at the very least in Option 2 (which is line 1. here).

[Nokia] We have issue with this LS.

“*UPIP shall be supported by the UE and the (ng-)eNB for all LTE bearers configured in EN-DC (Option 3 family), LTE/EPC (Option 1) and LTE/5GC (Option 5) regardless of the data rate from as soon as practical*. “

I think it will be confusing CT1 and RAN2 and not practical, particularly for Option3. For ngeNB, is total change of HW , ie radio and controller expected to support regardless of rate?

[Vodafone] I believe that those suggestions are practical in the network.

The text says “option 3 family…” and with option 3X the PDCP functionality is in the EN-DC capable gNB, so there would not be (and in real life, is not) any change of eNB hardware needed in this case.

The Vodafone proposal in S3-201305 describes extending the 3X concept to “option 1”, and again that would avoid hardware impact in the eNB.

[Qualcomm] Summary: Qualcomm would like this LS to be noted.

Motivation: Given the current status of UP IP discussion (unless something drastically changes in the last minute!) and based on the discussions re S3-201305 (where we think there are still some open issues that need to be further studied before LS is send to RAN2, assuming that Action 2 is related to this NR PDCP proposal), this LS should be noted.

[Ericsson] Regarding the working assumptions on UP IP, Ericsson just want to clarify that we don’t object to sending an LS to other groups.

[Vodafone] The purpose of this LS is to inform other groups of the progress of this meeting and it will be updated based on actual progress.

S3 201307  Draft LS to RAN and SA groups on UPIP is now available in the inbox for email approval.

Email approval deadlines

* Doc available:              18th of May      15:40 UTC
* Comments:                  20th of May      15:00 UTC
* Final version available: 21st of May      15:00 UTC
* Approval:                     22nd of May      15:00 UTC

[Mavenir] “To this end, SA3 has agreed a CR to 33.501 updating the requirement to use UPIP.”

Could you please point me to which tdoc this statement is referring to?

[Nokia] There was no such CR agreed which can address the points 1-5. Infact these points are HW/resource dependent, Iam not sure how configurations with legacy HW can support UP IP ‘regardless of data rate’.

Also it contains incorrect statements ‘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 ‘.

We cannot agree with this LS in the current form.

[Vodafone] @Mavanir - Sorry, I somehow missed the “draft\_” off the beginning of the file name

The latest version is now in the inbox as draft\_S3-201307 - Draft v1 - LS Out to RAN2 and CT1 on Updated User Plane Integrity Protection advice.doc

It no longer has the text you mention

@Nokia - There is a revision in the inbox as:  draft\_S3-201307 - Draft v1 - LS Out to RAN2 and CT1 on Updated User Plane Integrity Protection advice.docx

It does not have the text you mention – please review this and comment

[Mavenir] Thanks. Looks good to me.

[Vodafone] I revised it to v2 to delete the processing statement you did not like too…..

In the drafts folder as:  draft\_S3-201307 - Draft v2 - LS Out to RAN2 and CT1 on Updated User Plane Integrity Protection advice.doc

[Qualcomm] Qualcomm objects to sending this LS in its current form.

At the least, following changes need to be made:

* Delete para 2
* Delate para 3
* Delete the Note
* It is not clear to me what is the action to RAN2? I suggest RAN2 is removed.

It also seems to me that only CT1 and SA2 should be in the to list, given the scope of this LS.

I am also not sure whether v1 or v2 is the latest.

Please kindly provide v3 addressing the above issues so that I can review it again to see whether it is acceptable to us.

[Vodafone] Whilst I don’t see the reason for the deletion of these sections, they have been deleted as requested in v3.

Please review version 3 to see if you can accept the LS

@ Nokia – please also review this version to see if it acceptable to you.

[Qualcomm] Thanks for incorporating my comments.

I think ACTION 1) should be directed at both CT1 and SA2 (not just CT1).

Otherwise, v3 is fine for Qualcomm.

[Nokia] V3 is fine with us. Minor typo “S3-201391 (attached) - CR to TS 33.401 (LTE security) - Adds an~~d~~ informative reference to the ….  “

[Telecom Italia] I have the impression that the LS is just maintaining its original number “1307”, but its intended scope and  its concrete content is completely new, I would say “written from the scratch”.

RAN2 is also deleted from the target WGs, so this in another confirmation that the intended scope for this LS has been changed...

Sorry but I really fail to understand what is going on...

The original intention was to provide guidance to RAN2 and CT1 and now??

What is the CONCRETE purpose of this NEW LS, in regard of what SA asked SA3 to CONCRETELY do to solve the security issue raised by GSMA?

**Blockers:**

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

|  |  |  |
| --- | --- | --- |
| S3‑201310 | Cover sheet for TR 33.853 for Information  | VODAFONE Group Plc |

**Blockers: None**

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

|  |  |  |
| --- | --- | --- |
| S3‑201314 | pCR to 33.853 (UPIP) - Correction to Key Issue 5  | VODAFONE Group Plc |

[Vodafone] I have uploaded a revised version  draft S3-201314-r1  of this document to the Drafts folder.  This corrects an error in two places (one of which was existing text in TR 33.853, and one of which is new text proposed in this submission):

* the original text said that encrypted user plane data is “encrypted in counter mode (AES-CTR)”
* but that’s correct only for one of the standardized encryption algorithms, 128-NEA2
* so I’ve replaced this by more general text that captures the required point, “encrypted in a stream cipher mode”.

[Qualcomm] The key issue title for EPS does not seem to match the description of the key issue or the security threat/requirements.

If I understand correctly, with this key issue you want to study solutions for how HPLMN can control the use of UP IP in EPS, right? If so, I suggest that you change the title of 5.X to reflect it (e.g., Control of UP IP use by the HPLMN in EPS).

[Vodafone] OK, but in that case we should also change the title of key Issue #5 to e.g. “HPLMN Control of UP IP usage in 5GS” The two key issues are basically the same, i.e. how to move from optional/non-support in R15 to full support in the future. I’ll upload a rev 2 in a moment

[Samsung] Thank you for the r2. As the Key Issue 5 is based on TS 23.501 (Rel-15 and Rel-16), where the SMF determines the UP security policy (based on various criteria), let us not touch it.

Would like to suggest to make a new Key issue Y based on your modification to Key issue 5.

So that Key issue 5, has the security requirement

"The 5G system should support solution(s) to mitigate the threat mentioned in clause 5.5.3, when the integrity protection of a PDU session is not activated due to UE capability limitations or serving network policy."

and the new Key issue Y  will have

"The 5G system should support solution(s) to mitigate the threat mentioned in clause 5.5.3, when the integrity protection of a PDU session is not activated due to UE capability limitations or home network policy."

[Vodafone] The background to this change is that (in my understanding) the serving network policy is irrelevant in 5GS. In all cases, the HPLMN can set the Integrity Protection (and confidentiality) policy and this is either:

1. (with home routed roaming traffic) sent from the UDM to the h-SMF and on through the v-SMF to the AMF and RAN, or
2. (for non-roaming or local breakout of roaming traffic) sent from the UDM to the SMF and then onto the AMF and RAN (see fig 4.2.4-4 copied from TS 23.501 v16.4.0).

Section 5.10.3 “PDU Session User Plane Security” of TS 23.501 states:

“The SMF determines at PDU session establishment a User Plane Security Enforcement information for the user plane of a PDU session based on:

-              subscribed User Plane Security Policy which is part of SM subscription information received from UDM; and

-              User Plane Security Policy locally configured per (DNN, S-NSSAI) in the SMF that is used *when the UDM does not* provide User Plane Security Policy information.

-              The maximum supported data rate per UE for integrity protection for the DRBs, provided by the UE in the Integrity protection maximum data rate IE during PDU Session Establishment.”

If the UE is a legacy UE that does not support full rate UPIP, the HPLMN can know that from the IMEISV and so the HPLMN can set the UPIP policy in the UDM accordingly.

Overall, I remain very confused about what key issue 5 is trying to achieve in 5GS – it seems to have been drafted on the misunderstanding that security policy was determined by the VPLMN (which is the case in 2G/3G/EPC) and not by the HPLMN.

Potentially we need to ensure that the h-SMF is informed that the PDU session was rejected because the VPLMN doesn’t support full rate UPIP so that the HPLMN can steer the UE to a supporting VPLMN, but what else?

[Qualcomm] The difference between 5GC and EPS is that in the former we already support in R15 a way for home network to control the use of UP IP (therefore no need to study it in this TR) whereas in the latter we don’t have that support. I understood that is why are introducing new key issue for EPS to study solutions.

The existing key issue title is correct (as it is to look at solutions when UP IP is not in use for whatever reason). So, I think we should not change the title for the existing Key Issue 5.

[Vodafone] I’ve uploaded a rev 3 that restores the title of KI#5. However, now that the KI description is corrected, I have to say that I have no clue what KI#5 is trying to address.

[Qualcomm] R3 is fine for me. Thanks!.

**Blockers: None**

**Status at end of meeting (unless there are further comments): Approved (rev 3)**

|  |  |  |
| --- | --- | --- |
| S3‑201317 | Reduced overhead for UP IP for 5G RAN updates and conclusion  | Philips International B.V. |

[Ericsson] Ericsson objects to the recommendation in this contribution and proposes to note this contribution.

We don’t need to support an additional mechanism or solution for Option 2 based on solution #4.

[Vodafone] I have no objection to the solution refinements added in Change 1, but I don’t agree with Change 2, which concludes that this solution should be taken forward in normative work.  I haven’t seen enough support to justify that. So as it stands I would agree with Ericsson that the contribution should be noted.

[Philips International] Of course I would love to discuss more about the reduced overhead and other benefits of solution#4, and that we really should consider it going forward to provide the security protection that is needed against the aLTEr attack without affecting the data rates, but unfortunately we are running out of time for this meeting. I uploaded a revision to the document in the drafts folder ([S3-201317r1](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_99e/Inbox/Drafts/S3-201317r1.doc)) in which I removed change 2 with the update to the conclusion section. I hope with this change, the pCR is acceptable to you both and to everyone else.

[Vodafone] Thanks Walter.  This revised version is fine for me.

[Ericsson] The revised version is fine for me as well.

**Blockers: none**

**Expected Status at end of meeting (unless there are further comments): Approved (rev 1)**

|  |  |  |
| --- | --- | --- |
| S3‑201318 | Draft TR 33.853 v0.8.0  | VODAFONE Group Plc |

**Blockers: None**

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

|  |  |  |
| --- | --- | --- |
| S3‑201318 | Draft TR 33.853 v0.9.0  | VODAFONE Group Plc |

[Vodafone] This document is on email approval…

Email approval deadlines

•      Doc available:              18th of May      15:40 UTC

•      Comments:                  20th of May      15:00 UTC

•      Final version available: 21st of May      15:00 UTC

•      Approval:                     22nd of May      15:00 UTC

**Blockers: None**

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

# From Agenda Item 4.27:

|  |  |  |
| --- | --- | --- |
| S3‑201308 | draft WID - Normative changes for UPIP  | VODAFONE Group Plc |

[Vodafone] This document is on email approval:

Email approval deadlines

•      Doc available:              18th of May      15:40 UTC

•      Comments:                  20th of May      15:00 UTC

•      Final version available: 21st of May      15:00 UTC

•      Approval:                     22nd of May      15:00 UTC

DoCoMo asked to be added as a supporter

**Current Status: Under Discussion**

**Blockers: None**

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