**KI#2: Summary and way forward proposals**

(Volunteer: Ni Hui, Huawei)

1. **Summary of KI#2 status and companies’ views**
	1. **Solution Categories**

8 solutions are included in current TR. Based on protocols used for carrying metadata to UPF, solutions could be categorized as:

* Category #1: Media over QUIC (MoQ) based solutions (sol #9, #10)
* Category #2: UDP option based solutions (sol #11, #12, #27)
* Category #3: Proxying-UDP-in-HTTP based solutions (sol #24, #26)
* Category #4: GTP-U based solution (sol #25)
	1. **Summary of companies’ feedbacks**

13 companies provided feedbacks roughly follow on the above categories:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Company | Category #1: MoQ (sol 9,10) | Category #2: UDP option (sol 11,12,27) | Category #3: Proxying- UDP-in-HTTP (sol 24,26) | Category 4: GTP-U (sol 25) |
| Nokia | N (not mature) | N (Security) | Y? | N-  |
| Lenovo | N- (not mature, SA4 feedback needed) | N (Security, SA4 feedback needed) | Y | Y |
| Meta |  |  | Y |  |
| MediaTek | N- (not mature, SA4 feedback needed) | Y- (Security) | Y | Y |
| InterDigital |  |  | Y |  |
| Qualcomm | N- (not mature) |  | Y |  |
| Ericsson | N- |  | Y |  |
| vivo | Y |  | N- (Security etc.) |  |
| China Mobile | Y |  | N (not mature) |  |
| Futurewei | Generally not enough and may be challenging to resolve in Rel-19 |
| Huawei | Y |  | N (not mature) |  |
| China Telecom | Y | N | N |  |
| OPPO |  |  | N (not mature) | Y |
| Total | Y: 4N: 5 | Y: 1N: 3 | Y: 7N: 5 | Y: 3N: 1 |

Note: The above statistics are based on author’s reading to the companies’ comments and may be inaccurate.

**Observations:**

1. Both MoQ and Proxying-UDP-in-HTTP options got multiple supportive and negative feedbacks. Most negative feedbacks show the concerns on the matureness of related IETF work.
2. GTP-U and UDP options get less feedbacks comparing to the above options:
	1. GTP-U option: 4 feedbacks, main concern is related to the AS support.
	2. UDP option: 4 feedbacks, main concerns focus on security aspects.
3. Plenty of ENs exist in all of the options/solutions. (Category 1: 4 ENs, Category 2: 7 ENs, Category 3: 9 ENs, Category 4: 2 ENs)
4. 2 companies indicated that new (3?) solutions will be proposed in next meeting.
5. **Suggestions on way forward for SA2#162**
6. For each category, select one solution as baseline to merge the ideas, resolve ENs and address identified concerns.
7. Companies may consider whether to exclude solutions with very few supports.
8. Solutions (incl. potential new solutions) should be clear enough for evaluation after next meeting.
9. Re-evaluation should take place after next meeting.

# Annex. Companies’ view for KI#9

The following views were extracted from <https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_162_Changsha_2024-04/INBOX/DRAFTS/R19%20FS_XRM_Ph2>

|  |  |
| --- | --- |
| (2): end-to-end encrypted XRM (Sol #9, #10, #11, #12, #24, #25, #26, #27) | Nokia preferred approach is based on UDP-Connect from UE to AS. Nokia views that MoQ is not mature enough IETF and is too early for 3GPP. Nokia will not support non-secure solution such as UDP-option, ~~PDU set information in GTP-U headers~~. Sol #9, and Sol#10 are based on MoQ. IETF work is not complete and matured enough. Sol#11 complex solution on correlating QUIC and XRM metadata deviating from IETF protocol Sol#12. Better align with IETF/industry solution for security aspect. Sol#24: UDP-Connect (between UPF and AS) is feasible solution. Nokia will support.Sol#25: Adding PDU Set information over GTP-U (between AS and UPF) requires AS to support GTP-u and IPsec which may not take place in actual deployments.Sol#26 UDP-Connect (UPF and AS) is feasible solution. Nokia will supportSol#27: UDP-option is not secure. Lenovo] Solution#9 and 10 are based on MoQ scheme, which enables PSA UPF to acquire PDU set information via metadata as the MoQ relay. The MoQ is still in early stages in IETF and it is not clear yet whether MoQ is a suitable method to convey XR related media. 3GPP SA4 should also provide feedback on the feasibility of using MoQ for XR services. An LS should be sent to SA4 for feedback.Solution 11,12 and 27 are based on RTP over QUIC, which enables PSA UPF to acquire PDU set information via metadata/OFC contained in UDP-option. We see disadvantages with this option as any proxy in the path over N6 between the Application Server and the UPF could change/tamper with PDU set information which would impact handling of PDU-set in the RAN. An also should also be sent to SA4 on the feasibility of using UDP-Options to include PDU-set information as well as to SA3 to identify any security impacts.Solution#24, 25 and 26 are based on supporting a tunneled connection over N6 between th ePSA UPF and AS. Solutions 24 and 26 propose leveraging the Connect-UDP option where PDU set information is included within HTTP Datagrams whereas Solution#26 propose including PDU-set information within GTP-U header. Meta: We support the solution principles in Sol#26, or with Sol#24 with “6.24.3.2/Using Connect-UDP”. In addition, SMF may be configured with the information to establish “Connect-UPF” from UPF to AS proxy without receiving PCC rules from PCF. This is same principle for PDU set QoS in 23.501 … “the SMF may be configured to support PDU Set based QoS Handling without receiving PCC rules from a PCF.”[MediaTek] #9,#10 – Relates to MoQ, which is currently a draft standard. For MoQ to become popular, CDNs would need to adopt a new distribution mode and is therefore far into the future. The usefulness of MoQ would need to be explored by SA4 in the first instance.[InterDigital] We favor some form of a proxy based solution along the lines of solution #26.[Qualcomm] We are supportive of the option to send PDU Set information via the Capsule protocol using HTTP Datagrams (Solution 26). The concept of solution 9 (using a MoQ proxy in the UPF) is interesting but we think it is too early to conclude on this given that the related IETF work is still on-going.Ericsson: Following the principles shown below, we consider solutions #26 and #24 as our preferred ones, although solution #24 should not open the door to an indeterminate number of implementations based on SLA, see below.[vivo] The solutions on the table are more about customising the metadata format for PDU Set info in the external protocol, but they are not sufficient good, since it is 3GPP customised metadata format is probably not complied by OTT.#9#10 IETF defined MoQ metadata format e.g. object, group seems more suitable for the PDU Set info. #24 EN and #26 idea of using some HTTP proxy are not bad but the UE is not aware of interaction between and server and PSA UPF and the interaction cannot forbid the info which are sensitive to UE and bring in UE security concern. And the following need to be fixed. * #24: context ID doesn’t support the the new type metadata.
* #26: forwarding more only allow short header of QUIC cannot support the combination of the HTTP datagram and XRM payload in one UDP.

[China Mobile] Support to introduce MoQ into 5G system to let the UPF acts as relay node to identify the metadata, and the MoQ object format is alignment with the PDU set information.Solution 26 have big problem about the short header and the forwarding mode(which is conflict based on IETF). If not update, the solution 26 does not work.What’s more, the MASQUE is in the draft status in IETF, not mature. For Solution 24,Whether the Context ID can be updated to support PDU set information depending on IETF progress, and currently the RFC 9298 not support.  |
| Do you plan to submit a new solution for this KI? | [Nokia] we will submit a solution with UDP-connect starting from the UE because the UE is more suitable (than UPF) to know that an XRM app has started and a related UDP Connect to the AS is needed (The UPF cannot easily detect an XRM app due to traffic being ciphered)[Nokia] we are also planning to resubmit the IPSec based solution as an alternative.[Tencent] No[MediaTek] No[InterDigital] No.[Qualcomm] No.Ericsson: NoHuawei: No[vivo]yes[China Telecom] NoCATT:No[OPPO] No[China Mobile]No[Xiaomi]: No.[Samsung] No |
| What is your preferred conclusion (e.g. solution#, agreeable principles) for this KI? | [Nokia] IETF MASQUE based tunnelling (UDP-connect) based solution started from the UE (see above). Metadata defined in 3GPP (SA4)[Nokia] No MoQ based solutions as they are less generic and also less mature in IETF[Lenovo] Lenovo preferred option is to introduce a tunnelled connection over N6 between PSA UPF and AS, which enables PSA UPF to obtain PDU set information either via HTTP datagrams or GTP-U header, e.g., solution#24-26Meta: In general, we see the need to define a generic framework from this KI2 to carry additional information from UPF to AS and/or AS to UPF as defined is some solutions related to KI1/KI4/KI5/KI9. See response to these related KIs.[MediaTek] #24, 25 & 26, relate to delivery over a secure N6 tunnel. No strong view on what is encapsulated.[MediaTek] Or [MediaTek] #11,#12, #27 – Contingent on IETF/IANA approving a new set of UDP-options. The security concerns raised in the draft document, particularly regarding UDP options are not covered by DTLS (section 22), and protection against in-transit modification (section 15) needs to be addressed. [MediaTek] But not both (i.e., N6 tunnel or UDP-options)[InterDigital] Tunnelling based solutions along the lines of Solution #26.[Qualcomm] Solution 26.**Ericsson:** #26 and #24 can be merged.These are our agreeable principles:-Metadata needs to be integrity protected, but PDU Set information is not considered privacy sensitive. In addition, identification of the media fetched by an end-user should not be exposed (e.g. through MoQ track id) to avoid privacy violation. -Solutions putting additional requirements on the UPF not related with the goals of the key issue, such as implementing a MoQ relay should be avoided. -Solutions should be applicable to most use cases. We believe MoQ relay works for MoQ framework only.-Solutions based on any number of undefined implementation options (to be agreed by means of SLA), don't provide a basis for a standard. They are not acceptable to us. -Solutions should minimize impact on the UPF and Application Servers.[Futurewei] (revised 03/28) Solutions in KI#2 are not general enough that may be challenging to resolve in Rel 19 timeframe.Some principles:1. For encrypted communications and metadata, protocols, and mechanisms that different stakeholders (user, network operator, application provider) can accept explicitly should be considered.
2. Applications may serve different networks including mobile, Wi-Fi or fixed networks. Metadata to assist with QoS (in N6/IP network) should be possible to use across different access networks.
3. Protection of sensitive information and detection of modification (integrity protection) of any information on path is necessary. Traffic analysis of the metadata should reveal no additional information.
4. Metadata should be minimized to avoid leakage on path and reduce the amount of information revealed to trusted parties on path.
5. Encrypted side channel with metadata in a small packet can introduce significant overhead and delays. Mitigation of these costs should be considered.
6. Related to several points above, the process to standardize the metadata in the IETF (which is responsible for N6 protocols) and challenges related to the limited time to standardize for Release 19 should be considered a key factor.

[Huawei] Media over QUIC based solutions as described in sol#9 and sol#10 are preferred. No CONNECT-UDP (sol#24,#26) based solution, since it doesn’t support transmit the PDU set related info.Reasons: 1. It is preferred not to ask the application server to treat connections with clients from mobile network and fixed network differently, currently for an application service provider the vast majority (90+%) of the XR traffic are transmitted via fixed network, so from a deployment perspective, it would be hard to customize connections specifically for mobile network. MoQ solution(sol#9,10) deal with connections with clients from mobile network and fixed network uniformly, some other tunnel-based solutions like MASQUE tunnel(sol#24,26), GTP tunnel(sol#25), needs additional 3GPP customization from application server side.2. Avoiding additional encapsulation overhead to avoid MTU issue. In MoQ based solution(sol#9,10), no additional encapsulation is needed; in MASQUE tunnel(sol#24,26) and GTP tunnel solutions (sol#25) additional encapsulation header is added which may cause MTU issues.3. The metadata transmitted between UPF and AS should be protected with security, for the UDP option-based solution (sol#11, 12), additional security protection of metadata needs to be designed, or the solutions applies to the case with security domain between UPF and AS.4. If an IETF protocol allows extensions by other SDOs, then normally a vender specific extension with guidance on how the protocol can be extended will be provided, but for MASQUE tunnel protocol (e.g. Proxying UDP in HTTP, RFC9298), there is no such a vender specific extension, so for the MASQUE tunnel-based solution (sol#24,26), IETF extensions are missed.[vivo]There are many solutions on the table. Some feasibility issues are not fixed yet and too early to be considered in the conclusion. Hence, only the following agreeable principles are proposed 1. One possibility is Metadata can be provided by the server and is aware by the PSA UPF. The Metadata should be integrity protected and may be encrypted.
2. The mechanism should forbid the info which bring in security concern of the UE.
3. Only applied to DL traffic.
4. The metadata format supported by IETF is more preferred comparing to 3GPP customised metadata format with regards to the real usage in OTT.

[China Telecom]Maybe no solution is perfect. The UDP option related solution is not feasible and may have impact on SA3, therefore should first be excluded.For Sol#26, our concern is whether and how IETF standardization is required for HTTP proxy is hard to determine.For Sol#9 and Sol#10, since the metadata is always visible to relays, and each PDU Set can be well mapped to an Object of MoQ, we prefer this MoQ solution.[OPPO]The enhancements to the N6 GTP-U tunnel can be defined by 3GPP. As for the MASQUE tunnel protocol, IETF standardization is needed. Therefore, the N6 GTP-U tunnel based solution is preferred. Besides, we support the application server to have diversified choices. If any other N6 protocol is widely used by the applications and can be supported by the IETF, we can make it an option.[China Mobile]Support MoQ solution (9,10), and not acceptable for Solution 26(which does not work at current solution description), have problem for Slution 24 about how to update IETF RFC to let Context ID support PDU set information. |