|  |  |  |
| --- | --- | --- |
| **[S3-240223](https://protect2.fireeye.com/v1/url?k=b31249d2-d269e345-b313c29d-74fe4860001d-c2b375e222529273&q=1&e=989ae797-8ebd-4e4b-96a6-1adbdececeb7&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_115_Athens%2FDocs%2FS3-240223.zip" \t "_blank)** | Quantum Safe Cryptographic Protocol Inventory | ETSI TC CYBER |
| [**S3-240659**](https://protect2.fireeye.com/v1/url?k=708fb2b1-11f41826-708e39fe-74fe4860001d-64c8f30dfa4f1aaf&q=1&e=989ae797-8ebd-4e4b-96a6-1adbdececeb7&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_115_Athens%2FDocs%2FS3-240659.zip) | Discussion on Quantum Safe Cryptography Protocol Inventory | Ericsson |
|  | Ericsson (Mohsin): Presents the doc  Ericsson (John):  CMCC (Min Peng): SA3 don’t rely on IETF we refer to IETF so that sentence related to Quantum Key Distribution is not needed. Why to say that QKD is not practically a secure solution. Don’t agree with this statement.  Huawei (Zander): Discussion paper looks fine. LS reply can simply answer to the specific questions instead of providing additional comments/details which is not relevant to SA3 like whether the “Subject Public Key Info” correct or incorrect. Only answer to the questions relevant to SA3 should be captured. SA3 is not in position to state other additional stuffs.  CableLabs (Tao): Discussion paper is fine. We should not get into the details which are not related to SA3 which are little controversial. LS currently has too much information it needs to be simplified. Regarding SA3 activity related to PQC we need to discuss if we need additional work. Current TR (33.801) is generic, not exactly other working group is looking for what kind of work is to be done need to be discussed.  Chair: This discussion paper briefly mentions that, if IETF specifies it SA3 can adopt it  CableLabs (Tao): We need any additional work to be looked  Chair: We can tell the inventory to other WG. Do we know the inventory? Do we need another study for that?  Ericsson (John): Member of SA3 knows the inventory. Not sure if we need to make the list. Answer to the questions in LS needs to be positive, that is we are well aware of protocol and we are planning to make it quantum secure.  CableLabs (Tao): All industry is looking into it. SA3 needs to produce the inventory and show other WG to show that we are actively working on it  Ericsson (Mohsin): We should answer to the point we agree but we should also show that we are on top of what is happening. Our response should reflect that. We know the effect on algorithms, is it necessary to give inventory.  We should mention which algorithm is affected. We should have a systematic way to handle what other WGs are doing on PQC.  Chair: Hybrid Key Encryption algorithm, this is relevant to mobile/devices not sure if it is related to any study. Do we need any study to look into this?  Ericsson (Mohsin): Whether we need study it depends on companies. Ericsson preference is HPKE  CableLabs (Tao): We don’t need to say anything about HPKE in LS response. In discussion paper it is fine.  Chair: IETF Scope is wider internet, they may not consider mobile network constraints. They may not focus on UE/network node capability. When we adopt this hybrid scheme not sure if we can adopt without any concern.  CMCC (Fuwen): Encryption computation is high in mobile, not sure if this statement is reasonable solution or not.  Chair: IETF scope is generic. In their view this might be right in their approach whether this will fit into our mobile world that needs more attention from our side.  CableLabs (Tao): Agree with chair. Final reply LS should not this statement about HPKE, as it is not yet studied by SA3  Chair: In general we want to see opinion from all companies. Ericsson proposes that we need to reply with positive response and Huawei lists out some TRs/TSs or protocols |  |
| [**S3-240658**](https://protect2.fireeye.com/v1/url?k=482f0b0a-2954a19d-482e8045-74fe4860001d-1dc616d7fe8370a7&q=1&e=989ae797-8ebd-4e4b-96a6-1adbdececeb7&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_115_Athens%2FDocs%2FS3-240658.zip) | LS on Quantum Safe Cryptographic Protocol Inventory | Ericsson |
|  | Ericsson: Presents the LS response. Same as discussion. It is OK we don’t need to speculate what could be the solution but we should show that we are on top of the technology. Our reply should reflect that. Not sure if it is good approach to write inventory exhaustively maybe we can write principle.  Chair: Inventory should be for our own understanding not for external SDOs.  Agrees with Mohsin’s (Ericsson) proposal, we should show that we are adopting enhanced RFCs. This has LS has more details some companies don’t agree to have this much detail. We need to have a mix of both the reply LS for the final LS response.  Work in between Jeju meeting to have a merged LS response. Reply to specific question with less details  And also convey the message that we are watching we will take care of PQC migration in time aligning with 3GPP timeline.  Charter (Achari): Internally we need inventory otherwise we won’t know what should be our coverage  Chair: Zander and Mohsin to provide a discussion paper to show PQC way forward, by the august meeting  Huawei (Zander): Whether a session is needed in Jeju  Chair: No need to have a session. A discussion paper to show how SA3 will adopt the transition to PQC is needed. Ericsson’s discussion paper is a good base  Ericsson (Mohsin): We can have an internal document.  Chair: To know what should be our approach. Whether some separate study is needed or update sec profile. For Jeju meeting work together to have a single LS response capturing  Ericsson (Mohsin): It might be too tight to have a converged LS as we have less working time. Best approach could be to try to converge during meeting if we cannot manage before meeting. Not to take much time on floor.  CableLabs (Tao): Try to revise don’t submit original  Ericsson (Mohsin): we could massage our respective submission based on comments received  Huawei (Zander): We should respond in Jeju meeting |  |
|  | Draft reply from Huawei: [https://www.3gpp.org/ftp/Email\_Discussions/SA3/SA3%23116/PQC%20LS/S3-24xxxx%20draft%20reply%20LS%20to%20ETSI%20TC%20Cyber%20on%20QSC%20protocol%20Inventory.docx](https://protect2.fireeye.com/v1/url?k=7e0c015e-1f77abc9-7e0d8a11-74fe4860001d-62929e4078e7193a&q=1&e=989ae797-8ebd-4e4b-96a6-1adbdececeb7&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FEmail_Discussions%2FSA3%2FSA3%2523116%2FPQC%2520LS%2FS3-24xxxx%2520draft%2520reply%2520LS%2520to%2520ETSI%2520TC%2520Cyber%2520on%2520QSC%2520protocol%2520Inventory.docx) |  |
|  | Huawei (Zander): Presents  NIST (Jeff): Answer to Q5, is not related to Quantum cryptography work SA3 is taking care. So we don’t need to mention those.  Ericsson (Mohsin): Agrees with NIST, 256 bit algo work is not motivated by Quantum safe algorithm as mentioned in Ericsson’s LS response symmetric based is not under quantum threat. This discussion is too much on symmetric key.  Nokia (Stawros): Comparing both doc. Ericsson’s doc comments on material providing by ETSI Cyber QSC, that is ok but this is going towards conclusion assumption it’s a bit early, Huawei doc is from inventory perspective, that is fine, SA3 should provide inventory list for example for all rel-18 related work. Inventory should have complete view.  CableLabs (Tao): Likes how the LS is structured. But the content needs to be revised, it focuses too much symmetric key. |  |
| [**S3-240692**](https://protect2.fireeye.com/v1/url?k=c3c38eca-a2b8245d-c3c20585-74fe4860001d-4e9a655339363b20&q=1&e=989ae797-8ebd-4e4b-96a6-1adbdececeb7&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_115_Athens%2FDocs%2FS3-240692.zip) | LS on 3GPP studies for PQC Migration | GSMA |
|  | Chair : any comments on the document  CableLabs (Tao):We need some inventory  Huawei (Zander): GSMA doc they have done inventory work. It already lists 3gpp protocol affected by PQC  Nokia: has to aspects 1) methodology 2) explaining which algorithm which PCQ must be used. Kind of assessment.  One can look up to this doc to see which PQC algorithm to use  Chair: any negative comment?  CMCC (Fuwen): Doc has good point. This means system can be replaced by cypto algo easily. This means even if one algorithm is broken, then it can be replaced without many changes to the system this is good point  Chair: Action for SA3, 1) timeline of study spec and migration 2) legacy system considered for PQC migration? We should answer these questions |  |
|  | Draft reply from Huawei: [https://www.3gpp.org/ftp/Email\_Discussions/SA3/SA3%23116/PQC%20LS/S3-24xxxx%20draft%20reply%20LS%20to%20GSMA%20on%20PQC.docx](https://protect2.fireeye.com/v1/url?k=b31e1167-d265bbf0-b31f9a28-74fe4860001d-61b8e6b3c0b69aab&q=1&e=989ae797-8ebd-4e4b-96a6-1adbdececeb7&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FEmail_Discussions%2FSA3%2FSA3%2523116%2FPQC%2520LS%2FS3-24xxxx%2520draft%2520reply%2520LS%2520to%2520GSMA%2520on%2520PQC.docx) |  |
|  | Huawei: presents  Ericsson (Mohsin): part of comments has already been discussed. Symmetric algorithm are not impacted. 3GPP maintains only profiles for public key cryptography, SA3 has to wait for the SDOs to work on it.  Since symmetric key algorithm is to be left, what is left for legacy, legacy to use 128 bits, in our CP work if we update the profile it will automatically be applicable to 4G/3G. not ok to say we have no decision  CableLabs (Tao): why they ask timeline  Chair: They have been doing study for 2yrs or more. Very recently only NIST declared, symmetric algorithms are quantum safe. Question is on legacy, do we consider 4g/3g and what is the recommendation for migration. Discussion paper (for migration) should discuss this as well.  Nokia (Stawros): Don’t SA3 did anything here in these TSs/TRs. On legacy aspect this is operator view operator knows. From 3GPP perspective not sure if legacy term exists/ is relevant.  Chair: Consider legacy to be 4G/3G. Since 128 symmetric is considered safe then question is for SUPI encryption the vulnerability will continue as it is not addressed. Will we upgrade 4G and 3G specs for this?  Ericsson (Mohsin): In 4G/3G no SUCI mechanism that is independent topic. Only then question about PQC arises.  Chair: Existing vulnerabilities will continue for 4G/3G  Ericsson (Mohsin): Vulnerability exists. But it is not related to PQC discussion.  CableLabs (Tao): No SUPI encryption in 4G/3G there is no need for PQC migration. If any protocol is affected we may need to update profiles.  Chair: TLS or IPsec RFCs, when get enhanced, then we make it applicable for 3G and 4G  Apple (Ivy): First sentence is good. SA3 plan depends on will we consider symmetric key algorithm update for PQC even though PCQ not impacts symmetric key algorithm. If symmetric is also considered for PQC migration then we might have impact to 4G/3G. We need to decide if we only consider PQC impact to asymmetric or symmetric also.  We should make this clear that we just work on spec and not decided anything on migration. We don’t have any timeline for migration we only work on spec.  Chair: Symmetric are considered safe so we don’t need to list that in the context of this LS. Only asymmetric needs to be referred to.  This LS need to be modified based on the comments received.  Chair: We should prepare for migration discussion paper (for Maastricht meeting in Aug). |  |
| [**S3-240265**](https://protect2.fireeye.com/v1/url?k=516d059a-3016af0d-516c8ed5-74fe4860001d-b2d0dfb6e94c8477&q=1&e=989ae797-8ebd-4e4b-96a6-1adbdececeb7&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_115_Athens%2FDocs%2FS3-240265.zip) | LS regarding the publication of the Post Quantum Cryptography – Guidelines for Telecom Use Cases document in Feb 24 |  |