INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2025-2028

SG17-LS115

STUDY GROUP 17

Original: English

Question(s): 11/17 Geneva, 3-11 December 2025

Ref.: SG17-TD314R1/GEN

Source: ITU-T Study Group 17

Title: LS/r on informing about the latest PQTN TF publications (reply to GSMA-PQTN#93 Doc_003)

LIAISON STATEMENT

For action to: GSMA, 3GPP SA3

For information to: -

Approval: **ITU-T Study Group 17 meeting (Geneva, 11 December 2025)**

Deadline: End of May 2026

Contact: Arnaud TADDEI
Chair, ITU-T SG17
E-mail: arnaud.taddei@broadcom.com

Abstract: This liaison statement provides SG17 reply to GSMA-LS36 (SG17-TD40) on GSMA’s latest PQTN TF publications, with a particular focus on ITU-T Recommendations, notably the X.500 series, as well as addressing particular points raised by GSMA’s latest public document referred to in their LS.

ITU-T SG17 thanks GSMA for GSMA-LS36 for sharing GSMA’s latest PQTN TF publications. SG17 compared it with SG17’s work, in particular in its lead question (Q11/17) with a mandate on PQC.

Regarding GSMA’s Official Document PQ.03, ITU-T Study Group 17 would like to highlight the following points for GSMA ’s consideration:

- Under 3.4.1, the KEM algorithm Kyber is mentioned as the NIST selection. While Kyber had been selected by NIST and reflected initially as such in ISO/IEC JTC1 SC27 WG2 ongoing work, it is now a slightly different cipher, ML-KEM, in the FIPS-203 standard that finally got published last August.

SG17 notes that

- More recently, to provide a more secure, yet efficient alternative to ML-KEM, NIST selected HQC as an additional KEM to be standardized. HQC, like Classic McEliece, is a code-based KEM, which are generally considered to be more secure than lattice-based ciphers such as ML-KEM or Kyber, independently of the subtle differences between these ciphers of the same category.
- It is of note that SC27 WG2 recently started standardizing another lattice-based KEM, NTRU, as lightweight cryptography.
- Compared to Classic McEliece, HQC is more performance-oriented, which likely explains the choice made by NIST over draft ISO/IEC standard Classic McEliece, in a departure from NIST’s recent policy of following SC27, aligning more closely with the way the AES cipher was selected some two decades ago, where performance was the main criteria too, vs

the other two finalists of the AES competition, which had otherwise better security properties.
- HQC is expected to be published as a NIST standard in 2027.

Regarding 3.6.1 symmetric key sizes,

- SG17 is of the opinion that the ANSSI recommendation of 256-bit keys, which is in line with NIST IR 8105 - from 2016 yet still valid - represents the safe choice from a security standpoint.
- This is also the security level that SG17 recommends for quantum safety in ITU-T Recommendations such as X.1811, X.1197 Amd1 or X.510, based on the latest advances in quantum computing and its cryptanalytic applications that we are aware of.

SG17 is doing its best to keep adapting to and adopting the latest cipher standards and Recommendations as described above.

ITU-T SG17 looks forward to further collaboration, alignment and exchanging information with GSMA on this topic.