|  |  |  |
| --- | --- | --- |
| ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | SCV-TD116 |
| **SCV** |
| **Original: English** |
|  |  | Virtual, 3 June 2020 |
| **TD****(Ref.: SG13-LS134)** |
| **Source:** | ITU-T SG13 |
| **Title:** | LS/o/r on harmonization of term and definition of ‘key’ related to quantum-based security used in ITU-T SG17 and SG13 (reply to SG17-LS197) |
| **Purpose:** | Information |
| **LIAISON STATEMENT** |
| **For action to:** | - |
| **For comment to:** | - |
| **For information to:** | ITU-T SG17; SCV ; FG-QIT4N |
| **Approval:** | **ITU-T SG13 meeting (Geneva, 25 October 2019)** |
| **Deadline:** | N/A |
| **Contact:** | Gyu Myoung LEERapporteur of ITU-T Q16/13Korea (Rep. of) | E-mail: gmlee@kaist.ac.kr |
| **Contact:** | Leo LEHMANNChairman of ITU-T SG13Switzerland | E-mail: Leo.Lehmann@ties.itu.int |

ITU-T SG13 thanks SG17 for sending the LS on harmonization of term and definition of ‘key’ related to quantum-based security used in ITU-T SG17 and SG13.

Q16/13 reviewed definitions on the term “key” and the meeting agreed not to define the term “key” as the meaning of “key” is well described in clause 6.1 of draft Y.3800 (Y.QKDN\_FR) as follows.

*“A QKD protocol allows to distribute* ***symmetric random bit strings as a secure key*** *that can be proven to be secure even against an eavesdropper with unbounded computational resources under some assumptions supporting the security proof model.”*

Without the newly defined definition in clause 3.2 of Y.3800 (Y.QKDN\_FR), the NOTE on the term “key” in clause 3.2 is added as follows.

*“NOTE –In this Recommendation, "key" means "symmetric random bit strings" produced by QKDN.”*

Draft Y.3800 (Y.QKDN\_FR) might be revised to take into account the future progress of technologies and standardizations. Accordingly, if SG17 newly defines the term “key” later, SG13 will review it again to reflect the new definition.

Draft Y.QKDN\_KM is developing the several definitions of keys as follows;
- key data: Random bit strings in a key file, which are used as a cryptographic key.
- key management agent-key (KMA-key): Key data stored and processed in a key management agent (KMA).
- key supply agent-key (KSA-key): Key data stored and processed in a key supply agent (KSA).
- meta-data: Attribute information on key data and key management, such as key ID, key generation time, QKD device name, key size, key type (encryption key/decryption key, or seed key for symmetric cipher), relay time, and so on.
- quantum key distribution-key (QKD-key): Random bit strings generated by a QKD device, particularly referring to random bit strings before being resized and formatted in a KM.

These definitions refer to the functional architecture and key management functions which are specified in draft Y.QKDN\_Arch and draft Y.QKDN\_KM. Please note that these documents are on-going works and might vary based on the progress of the studies on QKDN in SG13.

For harmonization of terms and definitions used in QKD related work items, SG13 will closely coordinate with SG17 in the future.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_