|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ITU logo | INTERNATIONAL TELECOMMUNICATION UNION  **TELECOMMUNICATION STANDARDIZATION SECTOR**  STUDY PERIOD 2017-2020 | | | | SCV-TD110 | |
| **SCV** | |
| **Original: English** | |
|  | | |  | | Virtual, 3 June 2020 | |
| **TD**  **(Ref.: SG17-LS197)** | | | | | | |
| **Source:** | | | ITU-T Study Group 17 | | | |
| **Title:** | | | LS on harmonization of term and definition of ‘key’ related to quantum-based security used in ITU-T SG17 and SG13 | | | |
| **Purpose:** | | | Action | | | |
| **LIAISON STATEMENT** | | | | | | |
| **For action to:** | | | | ITU-T SG13; SCV | | |
| **For comment to:** | | | |  | | |
| **For information to:** | | | |  | | |
| **Approval:** | | | | ITU-T SG17 meeting (Geneva, 27 August - 5 September 2019) | | |
| **Deadline:** | | | | N/A | | |
| **Contact:** | | Heung Youl Youm  ITU-T SG17 Chairman | | | | E-mail: [hyyoum@sch.ac.kr](mailto:hyyoum@sch.ac.kr) |
| **Contact:** | | Dong-Hi SIM Associate Rapporteur of ITU-T Q4/17, SK Telecom | | | | E-mail: [donghee.shim@sk.com](mailto:donghee.shim@sk.com) |

ITU-T SG17 has identified that the term ‘key’ used in draft Recommendations related to quantum-based security in Q4/17 and Q16/13 requires harmonization, see details in Annex

SG17 propose to SG13 to harmonize the term ‘key’ and its definition across two SGs, with the assistance of SCV (Standardization Committee for Vocabulary) if appropriate.

**Annex:**

* Proposal to harmonize the term and definition of ‘key’ used in quantum related draft Recommendations in SG17 and SG13

**Annex**Proposal to harmonize the term and definition of ‘key’ used in quantum related draft Recommendations in SG17 and SG13

1. **Rationale**

**1.1 Definition of bit strings going from key management layer to service layer**

In C609 to SG17 Aug/Sep 2019 meeting, there is an editorial note making a point on the incoherence of the definition and use of the word ‘key’ in the draft recommendation X.sec\_QKDN-ov.

“**3.1.3**  **Key** [b-ETSI GS QKD 0014]: A key is a random digital data with an associated universally unique ID

*Editorial note: Shall we delete this definition as we did for Y.3800 or shall we define properly this concept of ‘key in the context of QKD networks? Note that the definition that we give from a ‘key’ is based on properties and parameters (randomness and identifier) which are different from the ones used by cryptographers (E.g. cryptographic key: A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm [*[*FIPS 201*](https://csrc.nist.gov/glossary/term/cryptographic-key)*] or secret key: A cryptographic key used by one or more (authorized) entities in a symmetric-key cryptographic algorithm; the key is not made public.[*[*NIST SP 800-133*](https://doi.org/10.6028/NIST.SP.800-133)*]). Should we create two definitions one for ‘cryptographic keys’ and the other one for ‘keys exchanged through QKD’?”*

However, in clause 3.1.1 of the document X-cf\_QKDN and in caluse 3.1.3 of the Appendix 1 from the same document, key is defined as below:

**“3.1.3 Key** [b-NIST SP 800-63-2] under Cryptographic Key: A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.”

In the ITU terms and definition database, we can find the following definition for ‘key’

|  |
| --- |
| **Term** : key |
| **Definition** : Parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot. |

This definition is very similar to the definition of ‘cryptographic keys’ that can be found in other SDOs. It looks quite reasonable to use ‘key’ for the random bit string that is delivered by the key management layer to cryptographic applications in the service layer.

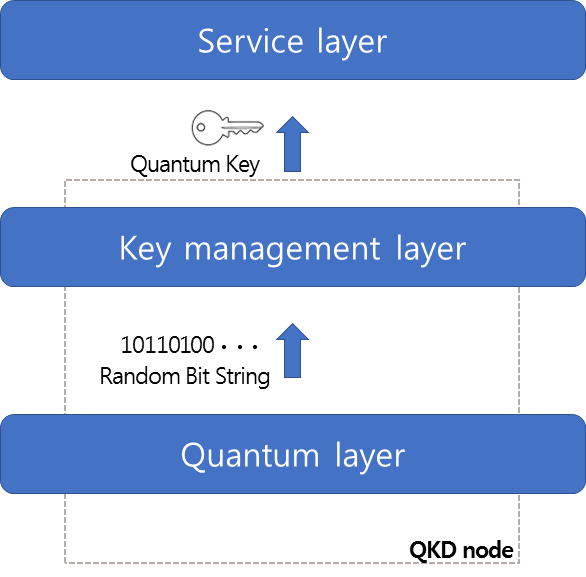
**1.2 Definition of bit strings going from quantum layer to key management layer**

In C713, KT Corp mentioned: “**Proposal 3**: For the Figure 1 in section 6 of AppendixⅠ, “Quantum Key” should be changed to “Random bit string” as this is what being transmitted from quantum layer to key management layer. Key should only be used when transmitted to Service layer as defined in 3.1.2.”

A screenshot of a cell phone

Description automatically generated

Figure 1 - Simple model for QKD networks (Q4-RGM-Shanghai-June-2019-Doc05(X.cf\_QKDN) )



Proposed Figure 1 - Simple model for QKD networks in C713

In SG13 Draft recommendation Y.QKDN\_KM, there is a definition for a ‘**QKD-key** [ITU-T X.sec\_QKDN\_km]: Random bit strings generated by a QKD device, particularly referring to random bit strings before being resized and formatted in a KM.’

Even though there is a wording for the key transferred from quantum layer to key management layer, we can find often the wording ‘key’ instead of ‘QKD-key’ in Y.QKDN\_KM. As an example in clause 7: “Pairs of QKD devices connected by a point-to-point QKD link constitute the quantum layer. Each pair generates **keys** in its own way. Generated **keys** are pushed up to KMs, and relayed via key management links.”

The discrepancy on the use of the word ‘key’ and its variations can be observed in all draft recommendations related to QKDN in SG17 and SG13. It is urgent to agree on a single term to define the bit string transferred from quantum layer to key management layer and another one for the bit string that goes from key management layer to service layer. Once, we agreed on these two terms with definitions, they shall be used in all work items dealing with QKDN with ITU-T.

This topic could be the first one for a collaboration between Q4/17 and Q16/13.

1. **Proposal**

We propose to use the same words and definitions for the concept of ‘key’ and other common concepts in QKDN work items with in ITU-T.

One possible way to move forward is to create one common glossary for QKDN work items within ITU-T.

SG17 agreed on this proposal and call for review by Q16 of SG13 in order to use the same glossary.

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