**Source: Ericsson**

**Title: Pseudo-CR on updating skeleton of clause 6**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: 0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This document proposes some content for clause 6 clause of the TR 33.703.

\* \* \* First Change \* \* \* \*

## 6.X Protocol #X

### 6.X.1 General

Editor’s Note: This clause includes background information about protocol #X (e.g., introductory information, relevant summary, if any, from the existing 3GPP profile of the protocol, useful references to specification documents etc.).

### 6.X.2 Current Work in IETF

Editor’s Note: This clause includes current status of PQC migration of protocol X in IETF — published RFCs, if any, and different drafts and their status. If Protocol X is specified by any other SDO than IETF, then the title of this clause will use the name of the appropriate SDO instead of IETF.

#### 6.X.2.1 IETF RFCs

#### 6.X.2.2 IETF Adopted Drafts

#### 6.X.2.3 IETF Non-Adopted Drafts

### 6.X.3 3GPP Considerations

Editor’s Note: This clause includes potential alternative options on PQC migration that 3GPP SA3 could consider. For example, for TLS 1.2, the following alternative options may be considered by 3GPP: (1) state in its profile that TLS 1.2 is expected to already have been fully phased out in 5G systems by XXXX date. (ii) add a note in its profile explicitly stating that TLS 1.2 is vulnerable to quantum attacks and is strongly recommended not to be used.

Editor’s Note: This clause does not include any conclusions.

\* \* \* End of Changes \* \* \* \*