INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2013-2016

COM 16 – LS 133 – E

English only

Original: English

Question(s): 3/16, 5/16 Seoul, 3 - 7 November 2014

LIAISON STATEMENT

Source: Q3/16

Title: LS on TLS and DTLS terminology [to 3GPPA SA3, IETF WG TLS, 3GPP CT4]

LIAISON STATEMENT

For action to: **3GPP SA3, IETF WG TLS**

For comment to: **-**

For information to: **3GPP CT4**

Approval: **Rapporteur Group meeting of Q3/16 & Q5 /16 (Seoul, Rep. of Korea, 7 November 2014)**

Deadline: **1 February 2015**

Contact: Christian Groves
Australia
Tel: +61 3 9391 3457
Email: christian.groves@nteczone.com

ITU-T Q3/16 works on support for the TLS and DTLS protocols in decomposed gateways using ITU-T H.248 as gateway control protocol. Initial support of these protocols is available, see published Recommendations ITU-T H.248.90 (10/2014) for TLS and ITU-T H.248.93 (10/2014) for DTLS. Initial support means that the (D)TLS protocols were modelled by so-called H.248 bearer connections (termed as "TLS bearer session" / "DTLS bearer session" in the Recommendations). These are abstractions, not necessarily equivalent to real (D)TLS sessions or (D)TLS connections, but sufficient for basic support by H.248 gateways.

However, additional support in the area of security and multiplexed protocol stacks ("WebRTC") imply a more precise model of TLS and DTLS protocol objects.

ITU-T Q3/16 would appreciate if you could provide clarifications particularly with respect to:

1. the distinction between *(D)TLS session* and *(D)TLS connection* (which implies a definition for each term, beyond the available descriptions / glossary from RFC side)
2. the *DTLS association* concept, e.g., is it equivalent to a DTLS session or DTLS connection or something in addition?
3. the *TLS renegotiation* procedure: what is the definition and at which level (TLS session or TLS connection level) does this procedure occur?
4. the *TLS resumption* procedure: what is the definition and relation to TLS renegotiation?

The location of TLS or DTLS endpoints in terminal and gateway equipment is slightly different due to the decomposition approach of H.248 gateways and their internal, hierarchical model of H.248 terminations and H.248 stream endpoints. Support of (D)TLS procedures (beyond the pure establishment and release) demand for the unambiguous detection of events (such as the

differentiation between TLS renegotiation and TLS resumption from TLS establishment). As part of the support of (D)TLS endpoints, the H.248 media gateways are able to determine the TLS profile and protocol capabilities via so called auditing capabilities procedures. However it is unclear which protocol capabilities are related to a (D)TLS session and (D)TLS connection and thus the MGC and MG may have different interpretations. The results of auditing TLS protocol capabilities and parameter values should be based on a common object model between the H.248 media gateway and its controller.

ITU-T Q3/16 is appreciative for your cooperation.

_____