INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2013-2016

COM 16 – LS 142 – E

English only

Original: English

Question(s): 3/16 Geneva, 9 - 20 February 2015

LIAISON STATEMENT

Source: ITU-T SG16

Title: LS/r on TLS and DTLS terminology – Follow-up comments and further questions for clarification (Ref: IETF No. 1379) [to IETF, 3GPP]

LIAISON STATEMENT

For action to: **IETF WG TLS**

For comment to: **-**

For information to: **3GPP SA3, CT4**

Approval: **ITU-T SG16 meeting (Geneva, 20 February 2015)**

Deadline: **8 June 2015**

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

ITU-T Q3/16 thanks you for your reply on our LS request (IETF No. 1379, our TD284/Gen). We would like to summarize our understanding by providing definitions and indicating some follow-up questions, which are related to (D)TLS protocol handling from the perspective of a decomposed gateway.

The text in italics relates to your reply. Follow-up questions are inserted:

Thanks for your questions about (D)TLS. What follows is a response to your questions; questions proceeded by Q# and answers by A#. If you have additional question please let us know.

Q1.

[What is] 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).

A1.

A TLS session is shared cryptographic state established by a full TLS handshake between two peers. The session's cryptographic state is used to establish the cryptographic key material for a TLS connection. A TLS connection is a transport relationship established between two peers that contains the cryptographic state to cryptographically protect data sent and received on the connection established through a full or abbreviated (session resumption) TLS handshake. A TLS session may span one or more TLS connections. Every TLS connection is associated with one TLS session. If session resumption (abbreviated handshake) is not used then the TLS session and TLS *connection will essentially be the same. A TLS session is identified by a Session ID in the client and server hellos. A TLS connection is usually identified by a host addresses and port numbers.*

Reply 1 (ITU-T):

a) **TLS session**: Thus, there is a "*TLS session cryptographic state*" object, which is shared by the two *TLS session endpoints* at client and server side. In our understanding the *TLS client session endpoint state* and the *TLS server session endpoint state* information largely overlaps (i.e., identical parameter-value pairs), but there is one additional parameter (the "*server address*") at client side. Is this correct?

Our understanding is that based on your description above "resumable TLS session" could be defined as follows:

Resumable TLS session:	The pair of a *resumable TLS client session endpoint state* and a *resumable TLS server session endpoint state*, coupled by the *TLS full handshake* procedure which was executed across the associated *TLS connection*.

b) **TLS connection**: the *TLS connection endpoints* at client and server side could be described by a n-tuple if the *TLS connection* represents a "transport relationship" according to your description.

c) **TLS connection identifier**: the following definition could be established based on your explanation ("*A TLS connection is usually identified by a host addresses and port numbers*"):

TLS connection endpoint identifier:	The local IP transport address and indication of "TLS/L4" protocol stack, i.e., the 4-tuple of {A_L, P_L, T, "TLS"} from the *TLS connection endpoint*. NOTE 1 – Parameter "L4" is required because TLS is a L4 independent protocol.

d) **Ratio** between **TLS session to TLS connection**: there is a ratio of 1:N.

e) **TLS session resumption**: according to your explanation, resumption is a) correlated with an abbreviated handshake and b) affecting the TLS connection, hence we might define:

TLS session resumption:	A TLS *session level concept* which represents the execution of a *TLS abbreviated handshake* procedure on an existing TLS session, i.e., a *semi-permanent TLS session*, for the purpose of either *deriving* a further *TLS connection* or *updating* of an existing *TLS connection*.

Q2.

The DTLS association concept, e.g., is it equivalent to a DTLS session or DTLS connection or something in addition?

A2.

The DTLS association is the same as a DTLS connection

Reply 2 (ITU-T):

Thanks for confirmation. We had the same interpretation based on the TLS related RFCs.

Q3.

The TLS renegotiation procedure: what is the definition and at which level (TLS session or TLS connection level) does this procedure occur?

Q4.

The TLS resumption procedure: what is the definition and relation to TLS renegotiation?

A3 and A4:

Resumption refers to the use of the state from an existing TLS session to establish a new TLS connection using an abbreviated handshake. During resumption the cryptographic parameters (algorithms etc.) remain the same. TLS renegotiation is the process of executing a new TLS handshake to establish new cryptographic parameters for a TLS connection (effectively a new TLS connection using the same host addresses and ports as the previous one). If the handshake is a full handshake then both a new session and a new connection are established and the renegotiated session may have different parameters.

Please note that session resumption and renegotiation are optional features; though TLS 1.2 recommended support for renegotiation; renegotiation was also updated by RFC 5746. Please note that TLS 1.3 is currently under development and these features are being reviewed.

Reply 3/4 (ITU-T):

In order to emphasize the difference between TLS session resumption and TLS session renegotiation, we would summarize your description as follows:

TLS session renegotiation:	A TLS *session level concept* which leads, - by the execution of a TLS handshake procedure (*full* or *abbreviated*) -, to the *update* of TLS protocol status information of an already established *TLS connection,* for the purpose of the establishment of new cryptographic parameters.

Could you please confirm or clarify our understanding? Q3/16 is appreciative for your cooperation.

____