WG TLS   Jens Guballa (ed.)
Internet Draft   Juergen Stoetzer-Bradler
Intended status: Informational   Alcatel-Lucent
Expires: September 2015

                                                  March 9, 2015

                  Terminology related to TLS and DTLS
                  draft-guballa-tls-terminology-00.txt

Status of this Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   This document may contain material from IETF Documents or IETF
   Contributions published or made publicly available before November
   10, 2008. The person(s) controlling the copyright in some of this
   material may not have granted the IETF Trust the right to allow
   modifications of such material outside the IETF Standards Process.
   Without obtaining an adequate license from the person(s) controlling
   the copyright in such materials, this document may not be modified
   outside the IETF Standards Process, and derivative works of it may
   not be created outside the IETF Standards Process, except to format
   it for publication as an RFC or to translate it into languages other
   than English.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF), its areas, and its working groups. Note that
   other groups may also distribute working documents as Internet-
   Drafts.

   Internet-Drafts are draft documents valid for a maximum of six
   months and may be updated, replaced, or obsoleted by other documents
   at any time. It is inappropriate to use Internet-Drafts as
   reference material or to cite them other than as "work in progress."

   The list of current Internet-Drafts can be accessed at
   http://www.ietf.org/ietf/1id-abstracts.txt

   The list of Internet-Draft Shadow Directories can be accessed at
   http://www.ietf.org/shadow.html

This Internet-Draft will expire on September 9, 2015.

Copyright Notice

Abstract

Purpose of this RFC is to provide a central place of all key terms as used by the various RFCs on protocols TLS and DTLS.

Table of Contents

1. Introduction

1.1. Background and motivation - Status of (D)TLS terminology

   The definition of the TLS protocol [RFC5246] is slightly unusual in
   the area of protocol specifications, because more like a software

description with a high-level data model, perhaps written after an
implementation. The RFC does not provide explicit definitions for
the main terms, rather providing a glossary in Appendix B/[RFC5246].
The Glossary itself provides descriptions of the main terms, but not
any definitions. At least not definitions at the detailed level as
required for protocol specifications, which implies a precise
linkage to objects as e.g. used within protocol and service data
units and protocol control information elements.

E.g., there are concerns and ongoing debates about the semantics of
some "handshake" related protocol procedures (catchwords "re-
establishment", "resumption", "renegotiation", "rekeying").
Associated to these procedural aspects is the underlying question
concerning the precise distinction between (D)TLS session and (D)TLS
connection level.

Without any doubt, TLS itself is a pretty successful, mature and
well-proven technology. The production of (D)TLS term definition
implies hence reverse engineering of (D)TLS RFCs.

1.2. Purpose

The purpose of this document is to provide a central place of key
terms as used in TLS and DTLS RFCs. The definitions should be
concise, but detailed enough from perspective of a protocol model,
and of course fully consistent and compatible with the existing
RFCs.

1.3. Scope

The focus is put on key terms which caused some controversy so far.

1.4. Disclaimer

Where there are discrepancies between this document and existing
RFCs on TLS and DTLS, the usage and "semantics" of these (D)TLS RFCs
take precedence over those described in this document.

2. Conventions used in this document

2.1. Prescriptive language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in RFC-2119 [RFC2119].

2.2. Notion of '(D)TLS'

The prefix '(D)TLS' indicate terms common to both protocols. The prefixes 'TLS' and 'DTLS' indicate protocol specific aspects.

2.3. Additional terminology

<term>:

   <definition>

2.4. Abbreviations used

AL   Local (IP) Address

AR   Remote (IP) Address

DTLS   Datagram Transport Layer Security

(D)TLS   DTLS or TLS

FQDN   Fully Qualified Domain Name

L4   (Protocol) Layer 4 (= IP Transport layer)

PL   Local (L4) Port

PR   Remote (L4) Port

RL   Record Layer

T   Transport (L4) protocol

TCP   Transmission Control Protocol

TLS   Transport Layer Security

UDP   User Datagram Protocol

3. Inventory of (D)TLS terms

3.1. Terminology related to endpoint entities

3.1.1. Term "(D)TLS endpoint"

   Definition:

      An instance of a (D)TLS protocol implementation with exactly one
      local IP (transport) address. A (D)TLS endpoint is housing one or
      multiple (D)TLS connection endpoints, which are acting either as
      (D)TLS clients or as (D)TLS servers (i.e., "(D)TLS client
      connection endpoint" and "(D)TLS server connection endpoint") when
      executing the (D)TLS handshake protocol.

   Reference:

      FIXTHIS

   Term relations:

      Definition based on terms "(D)TLS protocol implementation" (3.1.2.
      ), "(D)TLS client connection endpoint" (3.3.3.) and "(D)TLS
      server connection endpoint" (3.3.4.).

3.1.2. Term "(D)TLS protocol implementation"

   Definition:

      A (software or hardware) based implementation of the TLS protocol
      as specified in [RFC 5246] or of the DTLS protocol as specified in
      [RFC6347] (DTLS) and is always associated to a real system.

   Reference:

      None.

   Term relations:

      Definition based on term "real system" [ITU-T X.200].

3.2. Terminology related to session/connection entities

3.2.1. Term "(D)TLS connection"

   Definition:

A cooperative relationship among a pair of (D)TLS capable systems, represented by a (D)TLS client connection endpoint and a (D)TLS server connection endpoint (NOTE 1). A (D)TLS connection allows the execution of an establishment procedure given by either a (D)TLS full handshake or a (D)TLS abbreviated handshake (on request of the (D)TLS served user instance at (D)TLS client side). Thus, the mode of communication of the (D)TLS connection could be considered as connection-oriented (i.e., a (D)TLS connection is stateful, e.g., at the top-level by the 2-state model {IDLE, ESTABLISHED}).

Notes:

Thus, formally the (D)TLS connection is a set of two 8-tuples, refer to "(D)TLS connection endpoint".

Reference:

FIX THIS

Term relations:

Definition based on terms "(D)TLS protocol implementation" (3.1.2.), "(D)TLS client connection endpoint" (3.3.3.) and "(D)TLS server connection endpoint" (3.3.4.).

3.2.2. Term "Semi-permannt (D)TLS session"

Definition:

The pair of a semi-permanent (D)TLS client session endpoint state and a semi-permanent (D)TLS server session endpoint state, coupled by the (D)TLS full handshake procedure which was executed across the associated (D)TLS connection.

Reference:

FIX THIS

Term relations:

Definition based on terms "semi-permanent (D)TLS client session endpoint state" (3.4.8.), "semi-permanent (D)TLS server session endpoint state" (3.4.9.), "(D)TLS full handshake" (3.4.5.) and "(D)TLS connection" (3.2.1.).

3.2.3. Term "Transient (D)TLS session"

Definition:

The pair of a transient (D)TLS client session endpoint state and a
transient (D)TLS server session endpoint state, coupled by the
(D)TLS full handshake procedure which was executed across the
associated (D)TLS connection.

The transient (D)TLS client session endpoint state information and
transient (D)TLS server session endpoint state information is
immediately deleted after the successful (D)TLS full handshake
procedure.

Reference:

FIX THIS

Term relations:

Definition based on terms "transient (D)TLS client session
endpoint state" (3.4.10.), "transient (D)TLS server session
endpoint state" (3.4.11.), "(D)TLS full handshake" (3.4.5.) and
"(D)TLS connection" (3.2.1.).

3.2.4. Term "(D)TLS session"

Definition:

A semi-permanent (D)TLS session or transient (D)TLS session.

Notes:

Thus, a (D)TLS session is a transformed (D)TLS connection after
the successful execution of a (D)TLS full handshake procedure,
constituted by the pair of (D)TLS client session endpoint state
and a (D)TLS server session endpoint state. A (D)TLS session is
consequently an association between the two (D)TLS session
endpoints. The mode of communication of the (D)TLS session could
be considered as connectionless (i.e., a (D)TLS session is either
existing or not).

The nature of a (D)TLS session (from (D)TLS endpoint perspective)
is either volatile (i.e., the local (D)TLS session information
would be immediately discarded after a (D)TLS handshake procedure)
or semi-permanent (in case of resumable (D)TLS sessions).

Notably, a (D)TLS session may still exist after one or even both
(D)TLS connection endpoints, which did exchange the (D)TLS full
handshake messages from which the related (D)TLS session states
were derived from, are already destroyed.

The (D)TLS role (client or server) is a (D)TLS session level
characteristic. (to be confirmed)

Reference:

FIX THIS

Term relations:

Definition based on terms "(D)TLS semi-permanent session" (3.2.2.
) and "(D)TLS transient (volatile) session" (3.2.3.).

3.2.5. Term "DTLS association"

Definition:

Synonym to "DTLS connection".

Reference:

Term introduced by [RFC4347] and still used in [RFC6347].

Term relations:

Definition equal to "(D)TLS connection" (3.2.1.).

3.3. Terminology related to session/connection endpoint entities

3.3.1. Term "(D)TLS connection endpoint"

Definition:

A part of an instance of a (D)TLS protocol implementation, which
is able to send and receive (D)TLS messages, and which is
associated to exactly one 8-tuple being composed of

1) a creation point in time tc,

2) a destruction point in time td,

   3) a non-empty local IP address AL,

   4) a non-empty local L4 port PL,

   5) an empty or non-empty remote IP address AR,

   6) an empty or non-empty remote L4 port PR,

   7) a non-empty L4 transport protocol T, and

   8) the protocol string "TLS" or "DTLS".

Notes:

   If FQDNs are used as (D)TLS endpoint identifiers, then an
   additional requirement on the (D)TLS connection endpoint could be
   that AL is one of the IP addresses associated to the (D)TLS
   endpoint's FQDN.

Reference:

   FIX THIS

Term relations:

   Definition based on terms "(D)TLS protocol implementation" (3.1.2.
) and "(D)TLS message" (3.4.1.).

3.3.2. Term "(D)TLS connection endpoint identifier"

Definition:

   The local IP transport address and indication of "TLS/L4" or
   "DTLS/L4" protocol stack, i.e., the 4-tuple of {AL, PL, T,
   "TLS"/"DTLS"} from the (D)TLS connection endpoint.

Notes:

   Parameter "L4" is required because (D)TLS is a L4 independent
   protocol, hence a (D)TLS capable system could offer multiple
   (D)TLS endpoints with different L4 protocols.

Reference:

   FIX THIS

Term relations:

   Definition based on terms "(D)TLS protocol implementation" (3.1.2.
) and "(D)TLS message" (3.4.1.).

3.3.3. Term "(D)TLS client connection endpoint"

   Definition:

   A (D)TLS connection endpoint which sends a (D)TLS message
   containing a ClientHello handshake structure to another (D)TLS
   connection endpoint.

   Reference:

   The TLS ClientHello handshake structure is defined in [RFC5246]
   while the DTLS ClientHello handshake structure is defined in
   [RFC6347].

   Term relations:

   Definition based on terms "(D)TLS connection endpoint" (3.3.1.)
   and "(D)TLS message" (3.4.1.).

3.3.4. Term "(D)TLS server connection endpoint"

   Definition:

   A (D)TLS connection endpoint which receives a (D)TLS message
   containing a ClientHello handshake structure and subsequently
   sends a (D)TLS message containing a ServerHello handshake
   structure back to that other (D)TLS connection endpoint.

   Reference:

   The (D)TLS ServerHello handshake structure is defined in [RFC
   5246].

   Term relations:

   Definition based on terms "(D)TLS connection endpoint" (3.3.1.)
   and "(D)TLS message" (3.4.1.).

3.4. Terminology related to protocol procedures

3.4.1. Term "(D)TLS message"

   Definition:

     A unit of (D)TLS-RL user data as produced by the (D)TLS handshake
     protocol, the (D)TLS alert protocol or the (D)TLS change cipher
     spec protocol.

   Notes:

   Application Data are excluded from this definition.Reference:

     FIX THIS

   Term relations:

3.4.2. Term "(D)TLS client role"

   Definition:

     A (D)TLS connection endpoint is said to assume the (D)TLS client
     role, if it is a (D)TLS client connection endpoint.

   Reference:

     FIX THIS

   Term relations:

     Definition based on terms "(D)TLS connection endpoint" (3.3.1.)
     and "(D)TLS client connection endpoint" (3.3.3.).

3.4.3. Term "(D)TLS server role"

   Definition:

     A (D)TLS connection endpoint is said to assume the (D)TLS server
     role, if it is a (D)TLS server connection endpoint.

   Reference:

   FIX THIS

   Term relations:

      Definition based on terms "(D)TLS connection endpoint" (3.3.1.)
      and "(D)TLS server connection endpoint" (3.3.4.).

3.4.4. Term "(D)TLS message sequence"

   Definition:

      A finite sequence of (D)TLS messages.

   Reference:

      -

   Term relations:

      Definition based on term "(D)TLS message" (3.4.1.).

3.4.5. Term "(D)TLS full handshake"

   Definition:

      A (D)TLS message sequence where the first (D)TLS message contains
      ClientHello structure and if the sequence constitutes a successful
      (D)TLS full handshake message flow as specified in clause 7.3,
      Figure 1 of [RFC5246].

   Reference:

      [RFC 5246], clause 7.3, Figure 1

      Reference for DTLS?

   Term relations:

      Definition based on term "(D)TLS message" (3.4.1.).

3.4.6. Term "(D)TLS abbreviated handshake"

   Definition:

      A (D)TLS message sequence where the first (D)TLS message contains
      ClientHello structure and if the sequence constitutes a successful
      (D)TLS abbreviated handshake message flow as specified in clause
      7.3, Figure 2 of [RFC5246].

Reference:

[RFC5246], clause 7.3, Figure 2

Term relations:

Definition based on term "(D)TLS message" (3.4.1.).

3.4.7. Term "Data transfer ready (D)TLS connection"

Definition:

A (D)TLS connection after the successful execution of a (D)TLS
full handshake or a (D)TLS abbreviated handshake procedures.

Notes:

The notion of "DATA TRANSFER READY" refers to a specific state of
the (D)TLS connection and is synonym to the notion of
"ESTABLISHED". The general term "DATA TRANSFER READY" matches both
connectionless and connection-oriented type of connections, see
[ITU-T X.213 and X.214].

Reference:

-

Term relations:

Definition based on terms "(D)TLS connection" (3.2.1.), "(D)TLS
full handshake" (3.4.5.) and "(D)TLS abbreviated handshake"
(3.4.6.).

3.4.8. Term "Semi-permanent (D)TLS client session endpoint state"

Definition:

A (D)TLS client session endpoint state if its (D)TLS session
identifier value is non-empty.

Reference:

FIX THIS

Term relations:

Refer to "(D)TLS client session endpoint state" (3.4.12.) and
"(D)TLS session identifier" (3.4.20.

3.4.9. Term "Semi-permanent (D)TLS server session endpoint state"

Definition:

A (D)TLS server session endpoint state if its (D)TLS session
identifier value is non-empty.

Reference:

FIX THIS

Term relations:

Refer to "(D)TLS server session endpoint state" (3.4.13.) and
"(D)TLS session identifier" (3.4.20.

3.4.10. Term "Transient (D)TLS client session endpoint state"

Definition:

A (D)TLS client session endpoint state if its (D)TLS session
identifier value is empty.

Reference:

FIX THIS

Term relations:

Refer to "(D)TLS client session endpoint state" (3.4.12.) and
"(D)TLS session identifier" (3.4.20.

3.4.11. Term "Transient (D)TLS server session endpoint state"

Definition:

A (D)TLS server session endpoint state if its (D)TLS session
identifier value is empty.

Reference:

FIX THIS

Term relations:

Refer to "(D)TLS server session endpoint state" (3.4.13. 3.4.12.) and "(D)TLS session identifier" (3.4.20.

3.4.12. Term "(D)TLS client session endpoint state"

Definition:

The 17-tuple of following parameter-value pairs, as partially described in [RFC5246]:

TLS protocol parameter: Type:

1. version: ProtocolVersion

2. prf_algorithm: PRFAlgorithm

3. bulk_cipher_algorithm: BulkCipherAlgorithm

4. cipher_type: CipherType

5. enc_key_length: uint8

6. block_length: unit8

7. fixed_iv_length: unit8

8. record_iv_length: unit8

9. mac_algorithm: MACAlgorithm

10. mac_length: unit8

11. mac_key_length: unit8

12. compression_algorithm: CompressionMethod

13. master_secret: opaque[48]

14. session_id: SessionID (NOTE 1)

Other parameters: Type:

15. creation time tc: time (NOTE 2)

16. destruction time td: time

17. server_address: IPaddress (NOTE 3)

   Notes:

   1: A (D)TLS client session endpoint state is semi-permanent if and
   only if its session_id value is non-empty. Hence it is transient
   if and only if its session_id value is empty.

   FIX THIS: Session tickets [RFC5077] must be covered as well,
   reference to "(D)TLS session identifier" should be used.2: While a
   semi-permanent (D)TLS client session endpoint state's creation
   point in time correlates with the corresponding (D)TLS full
   handshake's end time (which is thus a point in time at which both
   TLS connection endpoints, which exchange the (D)TLS full handshake
   messages, do still exist), this semi-permanent (D)TLS client
   session endpoint state's destruction point in time is independent
   of the destruction points in time of these two (D)TLS connection
   endpoints. Especially, the semi-permanent (D)TLS client session
   endpoint state may still exist after one or even both (D)TLS
   connection endpoints are already destroyed.

   3: A (D)TLS protocol implementation may add further information to
   a (D)TLS client session endpoint state, like e.g. the associated
   (D)TLS server endpoint's source IP address. This additional
   information may be used by a (D)TLS client connection endpoint in
   order to decide if an already stored semi-permanent (D)TLS client
   session endpoint state may be used (may be "resumed") for the
   establishment of a new (D)TLS connection towards a destination
   transport address of another (D)TLS endpoint.

   Reference:

   [RFC 5246]

   Term relations:

   -

3.4.13. Term "(D)TLS server session endpoint state"

   Definition:

   The 16-tuple of following parameter-value pairs, as partially
   described in [RFC5246]:

        TLS protocol parameter: Type:

        1. version: ProtocolVersion

        2. prf_algorithm: PRFAlgorithm

        3. bulk_cipher_algorithm: BulkCipherAlgorithm

        4. cipher_type: CipherType

        5. enc_key_length: uint8

        6. block_length: unit8

        7. fixed_iv_length: unit8

        8. record_iv_length: unit8

        9. mac_algorithm: MACAlgorithm

        10. mac_length: unit8

        11. mac_key_length: unit8

        12. compression_algorithm: CompressionMethod

        13. master_secret: opaque[48]

        14. session_id: SessionID (NOTE 1)

        Other parameters (NOTE 3): Type:

        15. creation time tc: time (NOTE 2)

        16. destruction time td: time

     Notes:

        1: A (D)TLS server session endpoint state is semi-permanent if and
        only if its session_id value is non-empty. Hence it is transient
        if and only if its session_id value is empty.

        FIX THIS: Session tickets [RFC5077] must be covered as well,
        reference to "(D)TLS session identifier" should be used.

        2: While a semi-permanent (D)TLS server session endpoint state's
        creation point in time correlates with the corresponding (D)TLS

full handshake's end time (which is thus a point in time at which
both (D)TLS connection endpoints, which exchange the (D)TLS full
handshake messages, do still exist), this semi-permanent (D)TLS
server session endpoint state's destruction point in time is
independent of the destruction points in time of these two (D)TLS
connection endpoints. Especially, the semi-permanent (D)TLS server
session endpoint state may still exist after one or even both
(D)TLS connection endpoints are already destroyed.

3: Difference between the (D)TLS server session endpoint state
versus the (D)TLS server session endpoint: the 17th parameter
"server address" (refer to 3.4.12.) is of course missing at the
server side.

Reference:

  [RFC5246]

Term relations:

  -

3.4.14. Term "Resumable (D)TLS client session endpoint state"

Definition:

  Synonym for a semi-permanent (D)TLS client session endpoint state
  (3.4.8.).

Reference:

  -

Term relations:

  -

3.4.15. Term "Resumable (D)TLS server session endpoint state"

Definition:

  Synonym for a semi-permanent (D)TLS server session endpoint state
  (3.4.9.).

Reference:

   -

   Term relations:

   -

3.4.16. Term "Resumable (D)TLS session"

   Definition:

     Synonym for a semi-permanent (D)TLS session (3.2.2.).

   Notes:

     Expanded term: A (D)TLS session where the (D)TLS server session
     state as well as the (D)TLS client session state are both
     resumable. A (D)TLS session state is called resumable, if its
     (D)TLS session identifier value is non-empty.

   Reference:

     -

   Term relations:

     -

3.4.17. Term "Resumed (D)TLS session"

   Definition:

     A resumable (D)TLS session after the successful execution of a
     (D)TLS abbreviated handshake procedure.

   Notes:

     1: The (D)TLS session identifier value (of the resumed (D)TLS
     session) is identical to the previous value of the resumable
     (D)TLS session.

     2: The (D)TLS connection, which is established with the (D)TLS
     abbreviated handshake based on the existing resumable (D)TLS
     session, may be created while the original (D)TLS connection,
     which was established via the (D)TLS full handshake from which the
     resumable (D)TLS client and server session endpoint states and
     hence the resumable (D)TLS session were derived, is still

established, or only after this original (D)TLS connection is
already terminated.

3: Several new (D)TLS connections may be established using (D)TLS
abbreviated handshakes based on the same resumable (D)TLS session.
If the first (D)TLS connection is established using an (D)TLS
abbreviated handshake based on a resumable (D)TLS session, then we
may say that this (D)TLS session becomes a resumed (D)TLS session
at this first (D)TLS abbreviated handshake's end time.

Reference:

FIX THIS

Term relations:

FIX THIS

3.4.18. Term "(D)TLS session renegotiation"

Definition:

A (D)TLS session level concept which leads, - by the execution of
a (D)TLS handshake procedure (full or abbreviated) -, to the
update of the (D)TLS protocol status "connection-level"
information of an DATA TRANSFER READY (D)TLS connection, for the
purpose of the establishment of new cryptographic parameters.

Notes:

1: The initial (D)TLS full handshake or (D)TLS abbreviated
handshake is not regarded as a (D)TLS session renegotiation as
this handshake is executed on a (D)TLS connection which is in the
state IDLE. After this initial handshake is finished the (D)TLS
connection state is changed to DATA TRANSFER READY, and thus all
following (D)TLS full handshakes or (D)TLS abbreviated handshakes
on that (D)TLS connection are regarded as (D)TLS session
renegotiation.

2: The (D)TLS connection state remains in DATA TRANSFER READY
during and after the (D)TLS session renegotiation.

Reference:

FIX THIS

Term relations:

   FIX THIS

3.4.19. Term "(D)TLS session resumption"

   Definition:

   A (D)TLS session level concept which represents the execution of a
   (D)TLS abbreviated handshake procedure on an existing (D)TLS
   session, i.e., a semi-permanent (D)TLS session, for the purpose of
   either deriving a further DATA TRANSFER READY (D)TLS connection or
   updating of an existing DATA TRANSFER READY (D)TLS connection.

   Reference:

   FIX THIS

   Term relations:

   FIX THIS

3.4.20. Term "(D)TLS session identifier"

   Definition:

   A (D)TLS protocol parameter representing the identification
   allocated to a particular semi-permanent (D)TLS session.

   Notes:

   1: The definition is consistent and not redefining the explanatory
   description of a "session identifier" in the TLS glossary, as
   contained in Appendix B/[RFC5246].

   2: This definition may need to be extended by additional
   consideration of the session ticket based TLS session resumption
   mechanism as defined in [RFC5077]. There would be then two TLS
   protocol parameters (session_id and SessionTicket) as possible
   identifiers (both protocol parameters are mutually exclusive).

   Reference:

   [RFC5077]

   Term relations:

   Definition based on the term "semi-permanent (D)TLS session"
   (3.2.2.).

3.5. Colloquially used terms

This clause provides a list of terms which are not introduced, described or defined by (D)TLS RFCs, but sometimes used in discussions.

3.5.1. Term "(D)TLS session re-establishment"

Definition:

   -

Notes:

   There doesn't exist any definition so far.

Reference:

   None.

Term relations:

   Still open, dependent on definition.

3.5.2. Term "(D)TLS session rekeying"

Definition:

   -

Notes:

   There doesn't exist any definition so far (to be confirmed).

Reference:

   None.

Term relations:

   Still open, dependent on definition.

4. Security Considerations

FIXTHIS

5. IANA Considerations

FIXTHIS

6. References

6.1. Normative References

[RFC2119] RFC 2119 (03/1997), "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14.

[RFC5077] RFC 5077 (01/2008), "Transport Layer Security (TLS)
           Session Resumption without Server-Side State"

[RFC5246] RFC 5246 (08/2008), "The Transport Layer Security (TLS)
           Protocol, Version 1.2"

[RFC5746] RFC 5746 (02/2010), "Transport Layer Security (TLS)
           Renegotiation Indication Extension"

[RFC6347] RFC 6347 (02/2012), "Datagram Transport Layer Security
           Version 1.2"

6.2. Informative References

[ITU-T X.200] Recommendation ITU-T X.200 (07/1994), "Information
           technology - Open Systems Interconnection - Basic
           Reference Model: The basic model."

[ITU-T X.213] Recommendation ITU-T X.213 (10/2001), "Information
           technology - Open Systems Interconnection - Network
           service definition."

[ITU-T X.214] Recommendation ITU-T X.214 (11/1995), "Information
           technology - Open Systems Interconnection - Transport
           service definition."

Acknowledgments

<Add any acknowledgements>

Authors' Addresses

    Jens Guballa (editor)
    ALCATEL-LUCENT
    Lorenzstrasse 10
    D-70435 Stuttgart
    GERMANY

    Email: Jens.Guballa@alcatel-lucent.com

    Juergen Stoetzer-Bradler
    ALCATEL-LUCENT
    Lorenzstrasse 10
    D-70435 Stuttgart
    GERMANY

    Email: Juergen.Stoetzer-Bradler@alcatel-lucent.com

[7](). CHANGE LOG

[7.1](). Initial draft name "[draft-guballa-tls-terminology]()"

[7.1.1](). Version "-00"

   Following definition template is used:

     Term "<term>"

          Definition:
            <definition>.

          Notes:
            <comments, complementary information>

          Reference:
            <references>

          Term relations:
            <references to terms reused by this definition>

7.1.2. Changes against "-00"

   o #