[MS-TLSP]: Transport Layer Security (TLS) Profile

This topic lists the Errata found in [MS-TLSP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

Errata below are for Protocol Document Version V8.0 – 2015/10/16.

Errata Published*	Description
2016/02/22	In Section 1.2.1, Normative References, and Section 2.2.1, Client and Server Hello Messages, replaced all references to [IETFDRAFT-TLSHASH-03] with [RFC7627]. In Section 1.2.1, Normative References, changed from: [IETFDRAFT-TLSHASH-03] Bhargaven, K., Delignat-Lavaud, A., Pironti, A., Paris-Rocquencourt, Inria, Langley, A., and Ray, M., "Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension", draft-ietf-tls-session-hash-03, November 2014, https://tools.ietf.org/html/draft-ietf-tls-session-hash-03 Changed to: [RFC7627] Bhargaven, K., Delignat-Lavaud, A., Pironti, A., Paris-Rocquencourt, Inria, Langley, A., and Ray, M., "Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension", RFC 7627, September 2015, https://tools.ietf.org/html/rfc7627 In Section 2.2.1, Client and Server Hello Messages, changed from: Cipher suites and capabilities are negotiated as specified in [IETFDRAFT-TLSHASH-03]<3>, [RFC5246], [RFC2246], [RFC4492], and [RFC3268].<4><5><6> Changed to: Cipher suites and capabilities are negotiated as specified in [RFC7627]<3>, [RFC5246], [RFC2246], [RFC4492], and [RFC3268].<4><5><6>

* Date format: YYYY/MM/DD