draft-ietf-curdle-ssh-kex-sha2

Author: Mark D. Baushke <mdb@juniper.net>

Date: 2016-03-22

Status - draft-ietf-curdle-ssh-kex-sha2

- diffie-hellman-group14-sha256, diffie-hellman-group{16,18}-sha512
  - diffie-hellman-group{14,15,16}-sha256 (from an earlier draft) supported by multiple SSH implementations. In discussions, on the ietf-ssh@NetBSD.org list they seemed to agree in principal to dh-group{14}-sha256 and dh-group{16,18}-sha512
  - Damien Miller suggested dh-group14-sha256 and dh-group{16,18}-sha512 http://www.ietf.org/mail-archive/web/secsh/current/msg01176.html
  - Matt Johnston had preliminary support for Dropbear http://www.ietf.org/mail-archive/web/secsh/current/msg01119.html
  - Darren Tucker and Damien Miller have a patch for OpenSSH https://bugzilla.mindrot.org/show_bug.cgi?id=2515
  - IWAMOTO Kouichi in http://www.ietf.org/mail-archive/web/secsh/current/msg01139.html Support for dh-group{14,15,16}-sha256 in
    - RLogin http://nanno.dip.jp/softlib/man/rlogin/ 2.19.8,
    - Tera Term https://en.osdn.jp/projects/ttssh2/scm/svn/commits/6263
    - Poderosa http://poderosa.sourceforge.net/ in https://github.com/poderosaproject/poderosa/pull/17
- Key exchange deprecation - There seems to be agreement that the SHA1-based key exchanges be phased out. The table in the draft tries to provide reasonable guidance for implementations.