MD5 “flag out” for LDP
draft-nslag-mpls-deprecate-md5

- LDP currently uses TCP MD5 for authentication, which is no longer considered secure (see RFC 5925)
- Looking at TCP-AO + a yet TBD cryptographic mechanism as replacement
- Protocols and working groups that we’d like to coordinate with
  - BGP, MSDP, and PCEP
  - IDR, PIM, PCE, BESS, RTGWG, PALS and MPLS
  - Asking for guidance from Security Area
- Discussion takes place in the MPLS WG on Thursday morning.
- Hallway discussions welcome!