Conveying a Certificate Signing Request (CSR) in a SZTP Bootstrapping Request

draft-ietf-netconf-sztp-csr-01

Kent Watsen
Russ Housley
Sean Turner

NETCONF WG
IETF 109 (Virtual)
Since IETF 108

No updates.

• The original I-D was written to be ready for last call.

• There was an issue (next slide), but it resolved without needing to update this draft.

Oops, just posted -01

• To address an editorial comment left in -00’s Security Consideration section.
How to Support CRMFs (No Impact)

• The authors received a comment regarding support for CRMF (RFC 4211).

• Already the draft supports generating CSRs using CMP (RFC 4210) and CMC (RFC 5272), both of which MAY encode CRMFs.

• To address issues raised that are outside the scope of this draft:
  • draft-housley-lamps-crmf-update-algs
  • Algorithm Requirements Update to the Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)
  • draft-housley-lamps-cms-aes-mac-alg
  • Using the AES-GMAC Algorithm with the Cryptographic Message Syntax (CMS)
Comments, Questions, Concerns?

If not, then this draft is ready for WG Last Call.