draft-wouters-dane-openpgp-02

Paul Wouters <pwouters@redhat.com>

DANE - IETF89

draft-wouters-dane-openpgp-01 split in two

- draft-wouters-dane-openpgp-02 (RRtype format)
- draft-wouters-dane-openpgpkey-usage-00 (usage)

draft-wouters-dane-openpgp-02

- RDATA wire format binary RFC 4880 OpenPGP public keyring
- RDATA presentation format Base64 (similar to gpg –armor)
- Location: sha2-224(username)._openpgpkey.nohats.ca.
  - username hashing same as draft-ietf-dane-smime-06
  - hash only over username to support CNAME / DNAME
  - hash is not done for security or privacy

Call for WG adoption went out

draft-wouters-dane-openpgpkey-usage-00

- Scaffolding draft, needs your input
- Advise for MTAs, MUAs and Mail clients

Call for WG adoption went out

Running code

- Postfix and Sendmail milter plugin
  - ftp://ftp.nohats.ca/openpgpkey-milter (and github)
  - or yum install openpgpkey-milter
  - Deployed in production for paul@nohats.ca (bugs to paul@cypherpunks.ca)
- hashslinger extended with "openpgpkey" commandline tool
  - Create or verify DNS record from keys in GnuPG public keyring
  - creates OPENPGPKEY records in generic record or rfc format
  - http://people.redhat.com/pwouters/hash-slinger/ (and github)
  - or yum install hash-slinger