IETF 104 PRAGUE, MARCH 2019

TOM PUSATERI

PRIVATE SUBDOMAINS

SUBDOMAINS ON DEMAND

- private service discovery - requires authenticated, encrypted access
- user creates subdomain with trusted provider with established credentials like email address: pusateri@bangj.com => pusateri._pvt.bangj.com. Group: students._pvt.mit.edu
- user UPDATEs (FCFS) or uses out of band mechanism to install public KEY and/or TLSA record at apex
- all subsequent access requires signed query using private KEY and verified by trusted provider using public key
- updating/removing KEY or TLSA records ok with UPDATE signed with old private key
- Once <user>._pvt.<domain> added to client search domain, unicast service discovery works for private subdomain

ENCRYPTION / AUTHENTICATION

- All queries/responses MUST be done over TLS
- Server certificate can be verified with TLSA public key signed by DNSSEC
- service provider public key at apex of _pvt.<domain> used for response authentication
- response contains SIG(0) signed with providers private key, verified with public key
- client certificates can provide same authentication as SIG(0) signature if TLSA record present
- responses require SIG(0) signature (is TLS to authenticated server sufficient?)

FUTURE WORK

- -00 version used encrypted RRs, deprecated
- -01 version just uses TLS for encryption & SIG(0) for authentication
- Should we allow or require either KEY or TLSA public keys at <user> apex?
- Does use of _pvt break any leaf attribute rules?
- Is it ok to punt on compromised private subdomains and require out of band removal?
- Is requiring public/private key distribution amoung devices of <user> too difficult? Is it ok for the service provider to assist with this?
- Seperate READ/WRITE KEYS for Groups?
- Seperate signatures from encryption? (Tim Wattenberg & Willem Toorop)