DANE for STUN

Marc Petit-Huguenin
Olle Johansson
Gonzalo Salgueiro
2014/07/23
Context

- DANE for (D)TLS for STUN was discussed in London as part of the discussion about DTLS for STUN.
- It was decided to make it a separate draft to avoid delays to draft-ietf-tram-dtls-stun.
- Like ALPN, it is part of the same set of deliverables.
Operations

**IF** code implements this spec

**AND IF** it uses one or more DNS lookups

**AND IF** all DNS RRs from Source Domain to Host Name are DNSSEC secure

**AND IF** selected STUN protocol is secure (i.e., TLS or DTLS)

**AND IF** TLSA RR of Host Name is present and secure

**THEN** use TLSA to validate
STUN Usages

Only applies to:
- NAT Discovery Usage (RFC 5389)
- TURN Usage (RFC 5766)
- NAT Behavior Discovery Usage (RFC 5780)
Questions

- Milestone?
- Adopt as WG item?
- Reviews?