A Bootstrapping Procedure to Discover and Authenticate DoT/DoH Servers for IoT and BYOD Devices

draft-reddy-add-iot-byod-bootstrap-01

IETF 108

T. Reddy (McAfee)

D. Wing (Citrix)

M. Richardson (Sandelman Software Works)

M. Boucadair (Orange)

Agenda

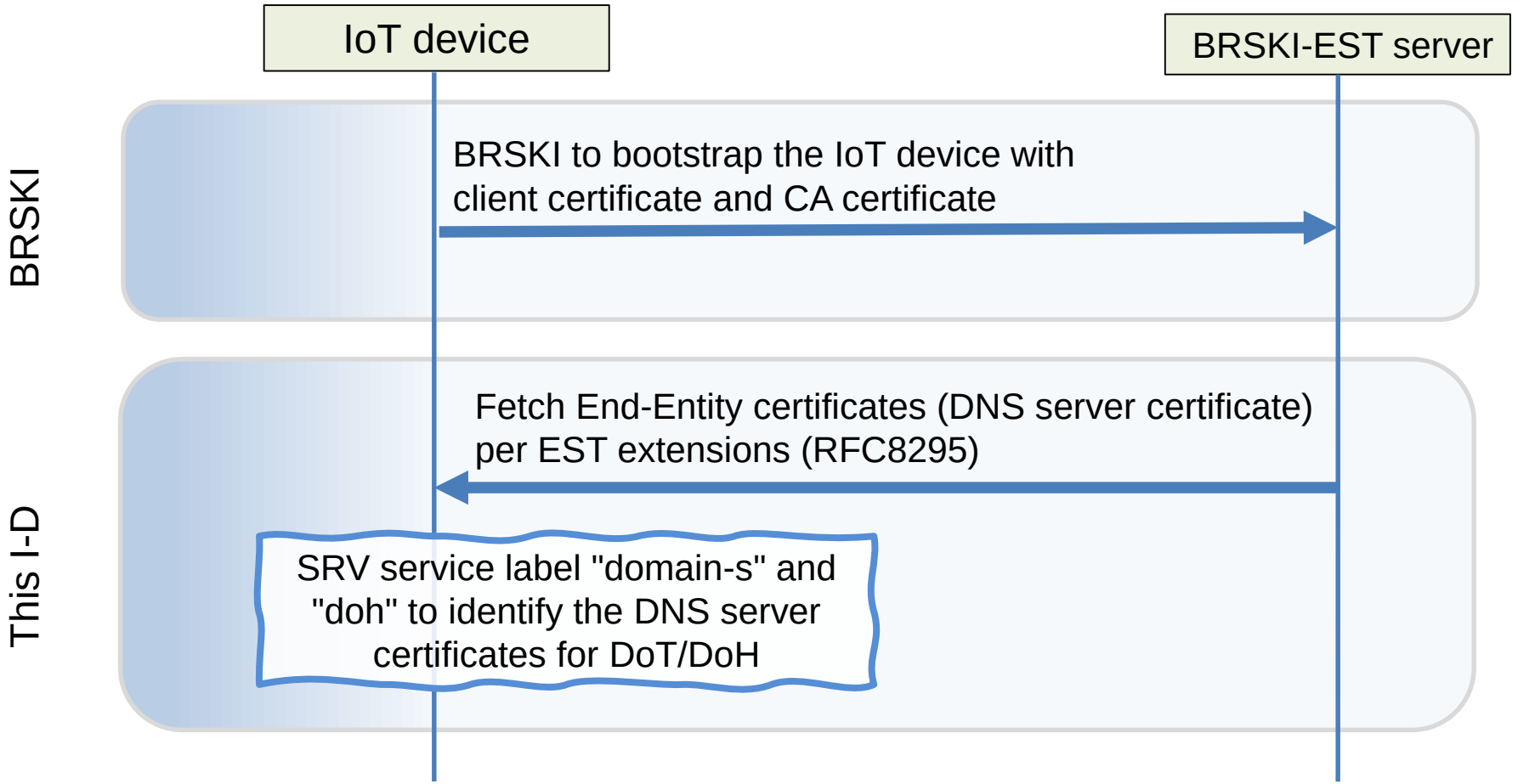
- Solution overview
  - Bootstrapping IoT Devices
  - Bootstrapping of BYOD Devices
- Connection handshake and DNS server certificate validation

Overview: Local DoT/DoH

- Secure Discovery and authentication of local DoT/DoH servers
- Scope: IoT devices and BYOD ("Bring Your Own Device") in Enterprise networks

- Motivation for local DoT/DoH
  - Manufacturer Usage Description (RFC8520) domain ACLs need DNS visibility
  - Block Malware
  - Local names (www-internal.example.com)

Bootstrapping IoT Devices



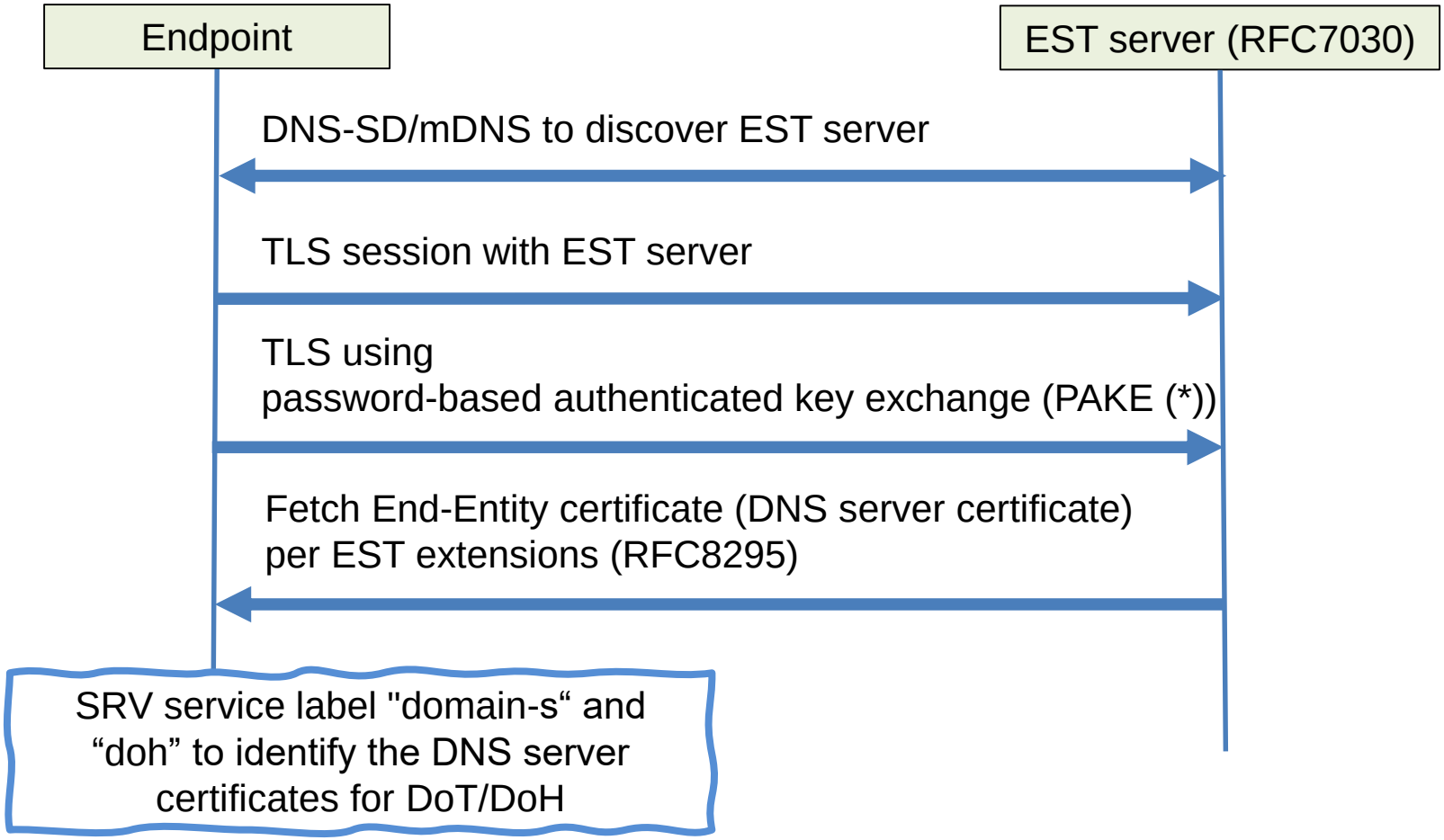
Bootstrapping Remote Secure Key Infrastructures (BRSKI), [draft-ietf-anima-bootstrapping-keyinfra]

DoH/DoT for BYoD Endpoints

- IT-owned devices are managed
  - Firefox Group Policy, Chrome settings, MDM, etc.
- BYoD are self-managed, so won't use:
  - MDM
  - Configuration Profile (e.g., Over-The-Air enrollment)
- This draft focuses on bootstrapping BYOD **without** MDM or configuration profile.

https://github.com/mozilla/policy-templates/blob/master/README.md#dnsoverhttps
https://www.chromium.org/developers/dns-over-https

Bootstrapping BYOD endpoints



(*) CFRG selected draft-haase-cpace and draft-krawczyk-cfrg-opaque

Connection handshake and DNS server certificate validation

- DoH/DoT server certificate MUST match DNS server certificate downloaded from EST server
- Validate the certificate using the Implicit trust anchor database entries
  - The DNS server certificate must pass PKIX certificate path validation
  - As required by EST (Section 3.2 of RFC8295)

draft-reddy-iot-byod-bootstrap-01

- Comments and suggestions are welcome

T. Reddy (McAfee)
D. Wing (Citrix)
M. Richardson (Sandelman Software Works)
M. Boucadair (Orange)