Bootstrapping Procedure to Discover and Authenticate DoT and DoH servers (20190724)

https://tools.ietf.org/html/draft-reddy-dprive-bootstrap-dns-server-04

IETF 105, Montreal

July 2019

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

Agenda

- Updates from 01 to 04 to address comments at IETF-104 meeting and ADD mailing list.
- Solution overview
  - Bootstrapping IoT Devices
  - Bootstrapping of endpoint Devices
- Discovery Phase
- Connection handshake and DNS server certificate validation Privacy and Security considerations
- Questions & Comments

Solution overview

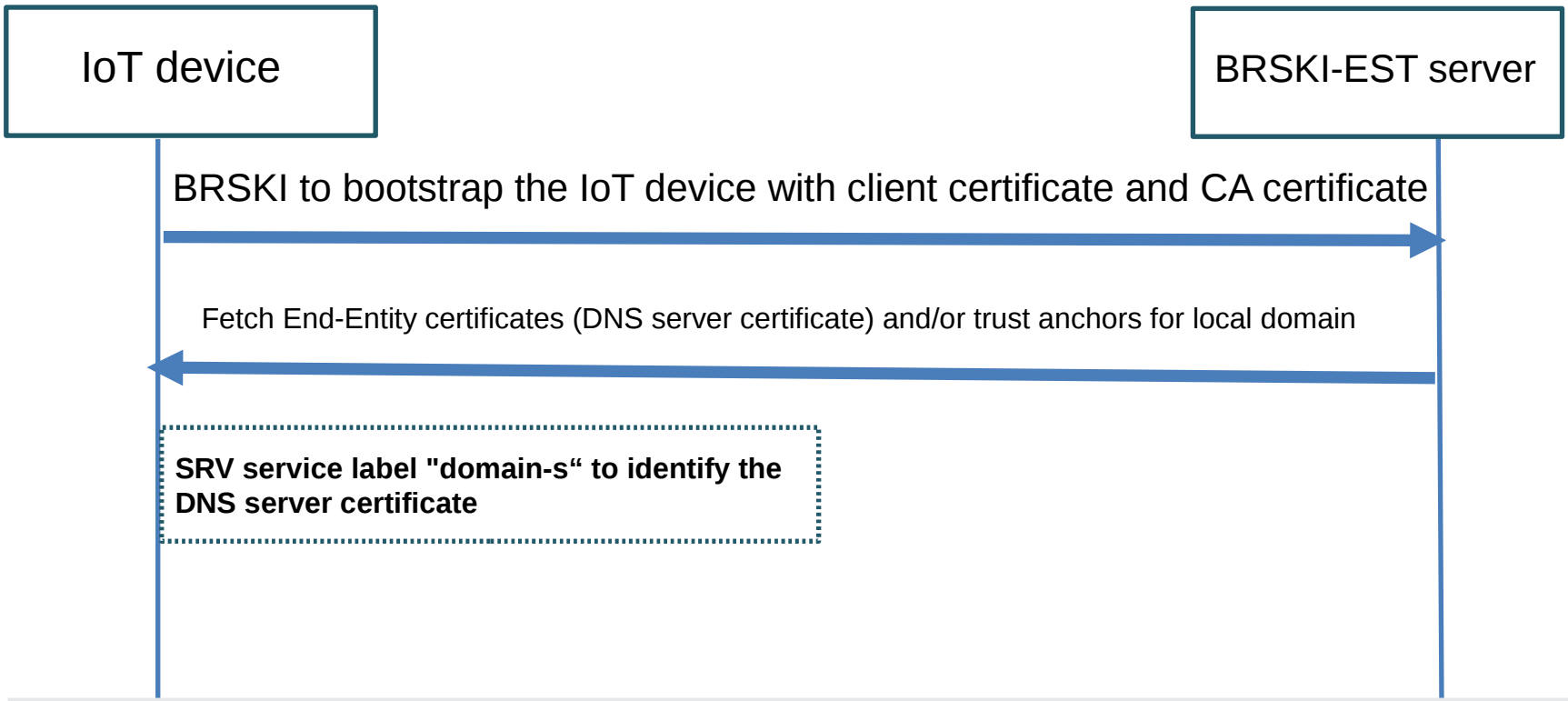
The draft discusses mechanisms to bootstrap endpoints to discover and authenticate local DNS-over-(D)TLS and DNS-over-HTTPS servers.

- **Scope is BYOD ("Bring Your Own Device") and IoT devices in Enterprise networks**

Why local DoT/DoH:

- **Manufacturer Usage Description RFC8520, failure to enforce ACL rules based on domain names**
- **Block Malware**
- **Local names (printer.local, nas.local, thermostat.local)**

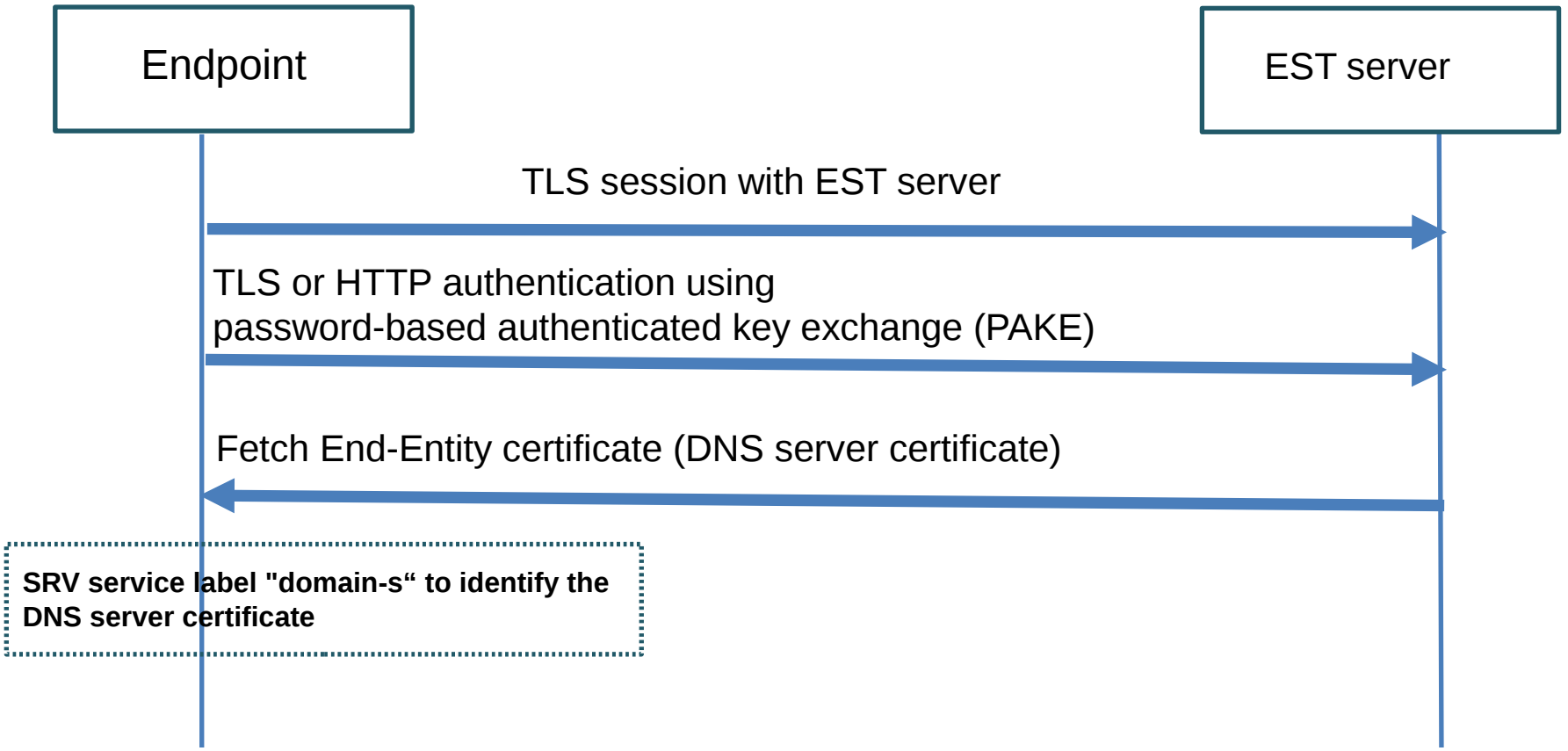
Bootstrapping IoT Devices



Bootstrapping Remote Secure Key Infrastructures (BRSKI) draft-ietf-anima-bootstrapping-keyinfra provisions credentials to access networks.

- BRSKI provides an automated mechanism for the bootstrap distribution of CA certificates from the EST server.

Bootstrapping of endpoint (BYOD) Devices



draft-barnes-tls-pake-04 (Usage of PAKE with TLS 1.3) or draft-sullivan-tls-opaque-00 (Usage of OPAQUE with TLS 1.3) *Note: PAKE integration in TLS is discussed in CFRG*
RFC8120: Mutual Authentication for HTTPS
RF7030: Enrollment over Secure Transport

Discovery Phase

- S-NAPTR lookup to learn DoT and DoH protocols supported by the DNS server and the DNS privacy protocol preferred by the DNS server administrators

```
example.net         IN NAPTR 100 10 "" DPRIVE:dns.tls  "" dns1.example.net.
                    IN NAPTR 200 10 "" DPRIVE:dns.dtls "" dns2.example.net.

dns1.example.net.   IN NAPTR 100 10 S DPRIVE:dns.tls "" _domain-s._tcp.example.net.

dns2.example.net.   IN NAPTR 100 10 S DPRIVE:dns.dtls "" _domain-s._udp.example.net.

_domain-s._tcp.example.net.       IN SRV   0 0 853 a.example.net.
_domain-s._udp.example.net.       IN SRV   0 0 853 a.example.net.

a.example.net.         IN A         192.0.2.1
```

Discovery Phase

- If DNS-over-HTTPS protocol is supported by the DNS server, discover the URI templates using the mechanisms discussed in “Associating a DoH server with a resolver”
  - (draft-sah-resinfo-doh-00).

Connection handshake and DNS server certificate validation

- Match the certificate in TLS handshake with the 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

Privacy considerations

- A new privacy certificate extension that identifies the privacy preserving data policy of the DNS server. (a policy tool)
- Listing some of them
  - User identity is logged or not and logging duration
  - Logging duration of transaction data
  - Blocks domain resolution of certain domains (e.g. malicious). Logging period for access to malicious domains blocked.
  - Transaction data shared with partners or not and names of partners.
  - URL that points to security assessment report of the DNS server by a third party auditor.

Security considerations

- User can enable the discovery mechanism in trusted networks.
- If the user trusts the network, the user can enable strict privacy profile with the DNS-over-(D)TLS or DNS-over-HTTPS server discovered in the network.

draft-reddy-dprive-bootstrap-dns-server-04

- Comments and suggestions are welcome