Securing Ancillary Data for Communication with Devices in the Network

Abhishek Tiwari

IETF 118, Prague

Motivating use cases

Some motivating problems:

- Can the CSP inform the CAP on which video sessions to self limit based on subscriber's plan details?
- Can the CSP inform the CAP on which video sessions to self limit based on the congestion of the serving cell that the subscriber is attached to?
- With QUIC, TLS 1.3 and Encrypted Client Hello (ECH) it is getting harder and harder for CSPs to classify the traffic flowing through their network. Is it possible for the CAPs to tell the CSP what kind of Quality of Service is important for the traffic in a session?
    - E.g. is it a latency sensitive application? What priority, burst size and packet delay budget the application desires?
- Can CSPs send telemetry or throughput guidance to CAP applications to assist the estimation and control loops running at CAP server/client.

CSP: Communication Service Provider
CAP: Content and Application Provider

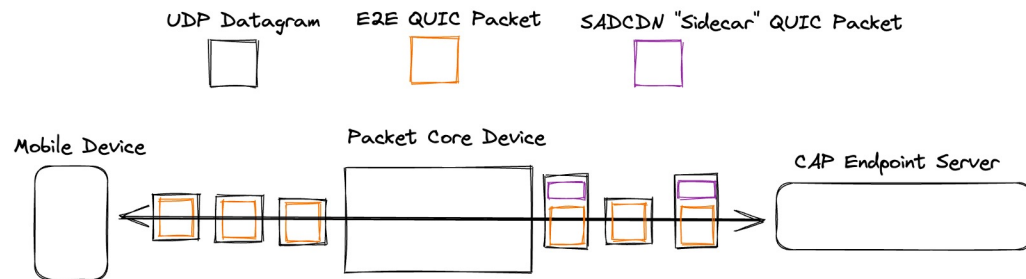# Securing Ancillary Data for Communicating with Devices in the Network (SADCDN)

Two key design considerations

1. **An In-band interface:** An In-band interface simplifies the association of the shared metadata with the flow/session that the metadata applies to.
2. **Security:** The privacy and integrity of the metadata must be guaranteed.

SADCDN solution sketch and status
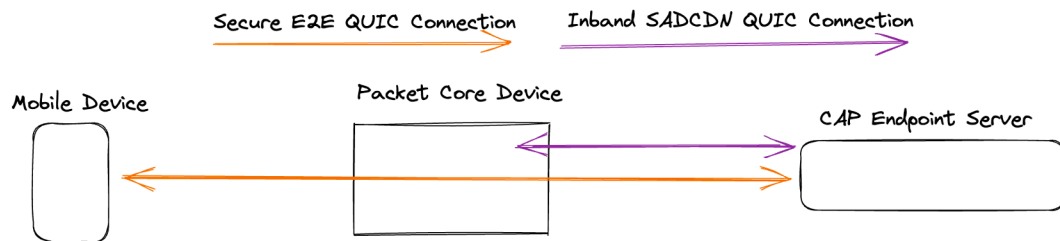
The two connections have completely independent cryptographic contexts

SADCDN draft was presented at IETF 117 dispatch session.

Draft: https://datatracker.ietf.org/doc/draft-joras-sadcdn/

Slides from IETF 117: https://datatracker.ietf.org/meeting/117/materials/slides-117-dispatch-sadcdn-00.pdf

Next Steps Discussion

1. Create a mailing list

1. Birds of Feather at IETF 119

1. Interim meeting to narrow down the scope / charter of the working group