DISPATCH/
SECDISPATCH
@IETF124

Customer Facing Relay: Source Privacy in Encrypted Transport

draft-scalone-cfr-source-privacy-00

Gianpaolo Angelo Scalone – Vodafone Group

Customer Facing Relay: Source Privacy in Encrypted Transport

Current Situation:

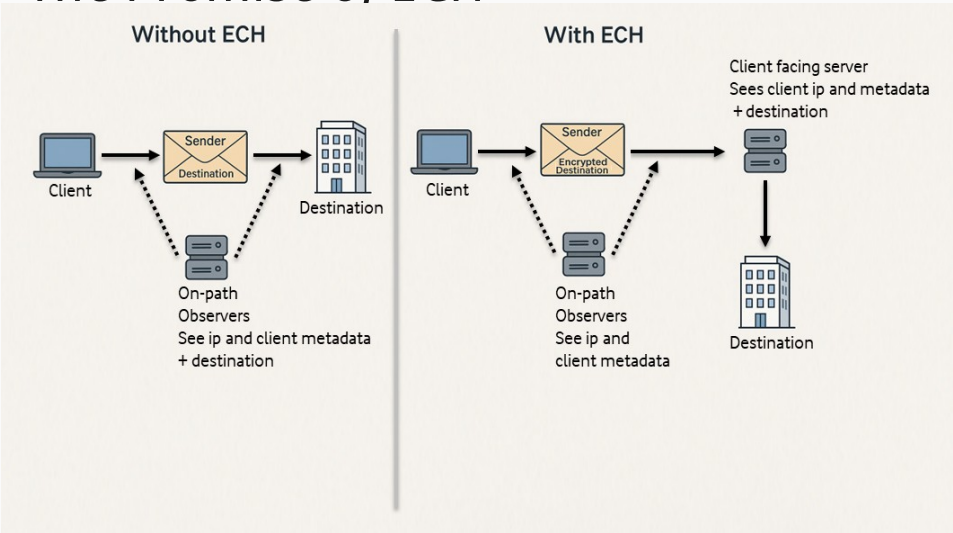
- **TLS 1.3 and ECH** improve privacy by hiding what users access, but not who.
- **CDNs and hosting providers** still see client IPs and can correlate across domains.

Customer-Facing Relay (CFR)

- **Lightweight relay at the network edge** (ISP/Enterprise).
- **Separates user identity from destination**, reducing metadata correlation.
- **Complements ECH** by protecting the traffic source — enhancing end-to-end privacy.

Background

The Promise of ECH



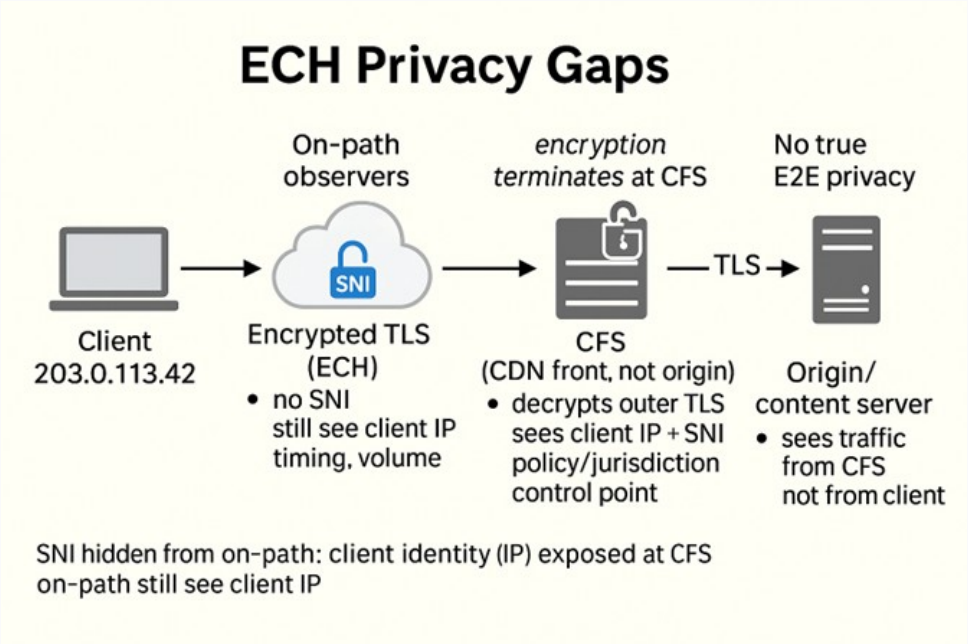
To provide destination privacy – protecting users against network-level tracking and censorship by encrypting TLS handshake metadata

- Encrypts the TLS ClientHello
- Protects Server Name Indication (SNI)
- Hides the final destination from on-path observers
- more privacy respect legacy TLS

The remaining gaps - Privacy

*Client Facing Server (CFS) acts like an "**ISP of content providers**":*

- *Handles **ECH** for large domain sets*
- *Sees both **client IP** and **destination domain**, enabling correlation*

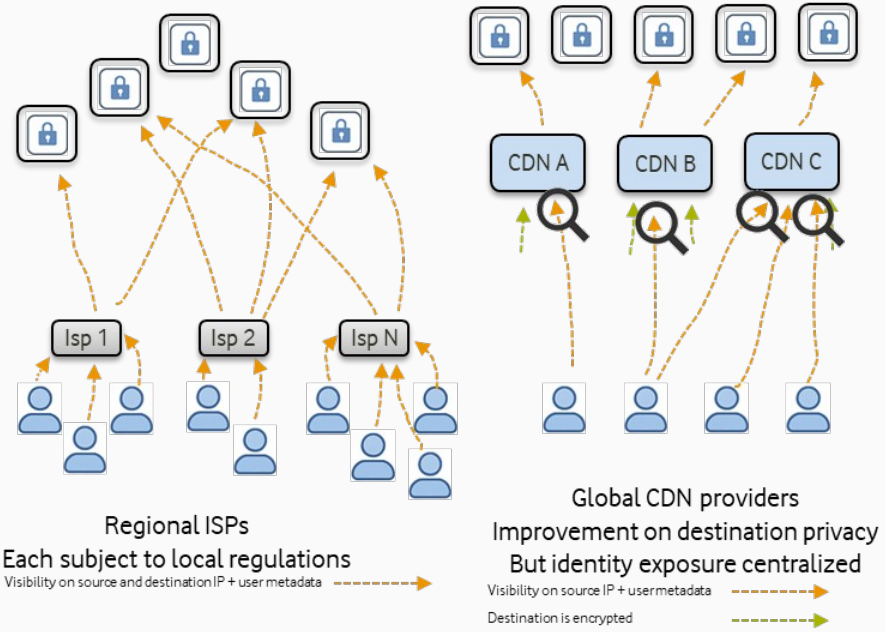


The remaining gaps - Centralization

Jurisdictional mismatch: ***CDNs centralized, users worldwide***

risks:

- *Local law* ***compliance***
- *Foreign surveillance* ***exposure***



Internet moves from decentralized to few control points

proposed solution

ECH: Progress, but Gaps Remain

Open Issues

- *Protecting client identity (IP, metadata)*
- *Reducing centralization and single points of control*

Possible Mitigations

- *CFR approach*
- *GDPR like approach*

Request to DISPATCH

Seek feedback on the privacy gap and proposed architecture and identify the most suitable venue for further work