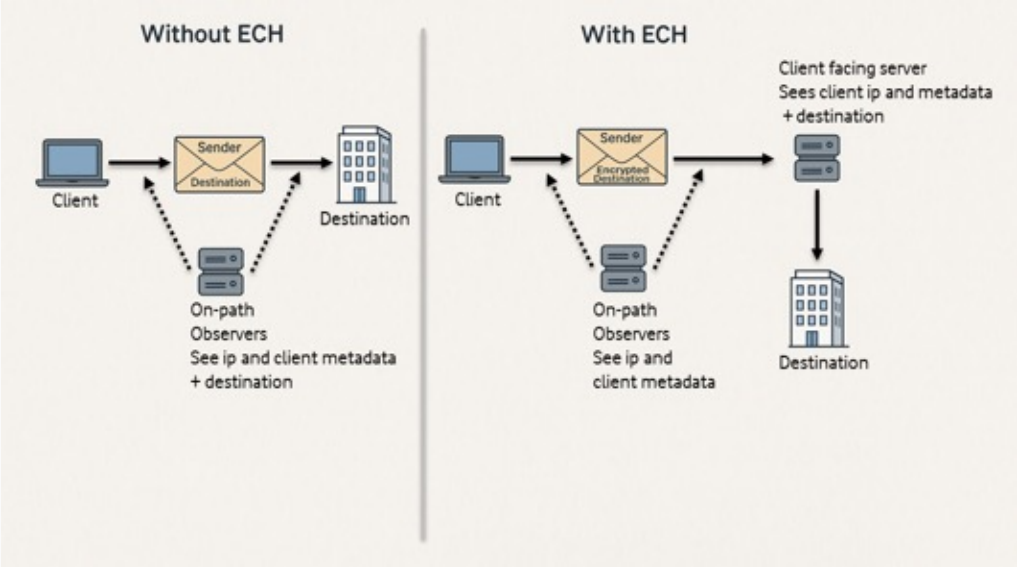
DINRG @IETF124

Beyond ECH: Architectural Directions for Source Privacy and Decentralization.

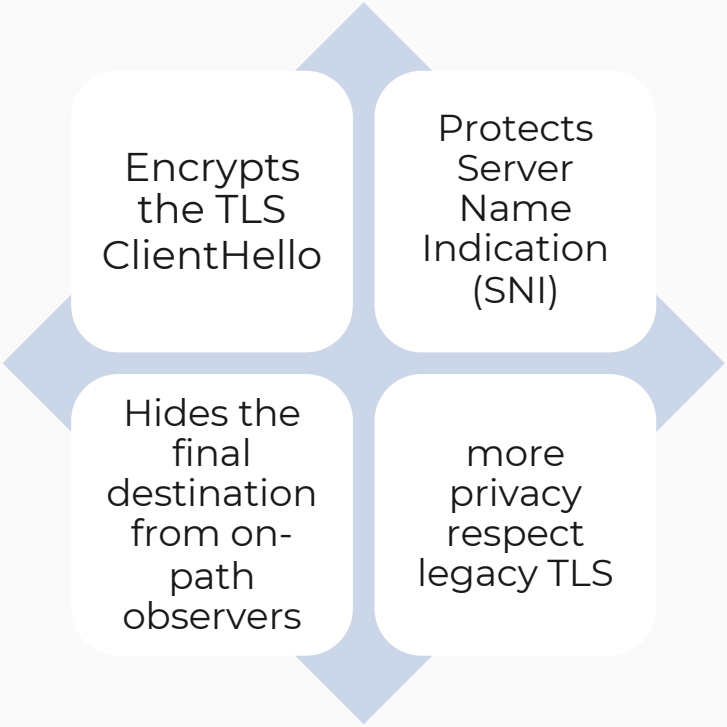
Gianpaolo Angelo Scalone – Vodafone Group

Introduction – ECH Privacy Gains

The Promise of ECH



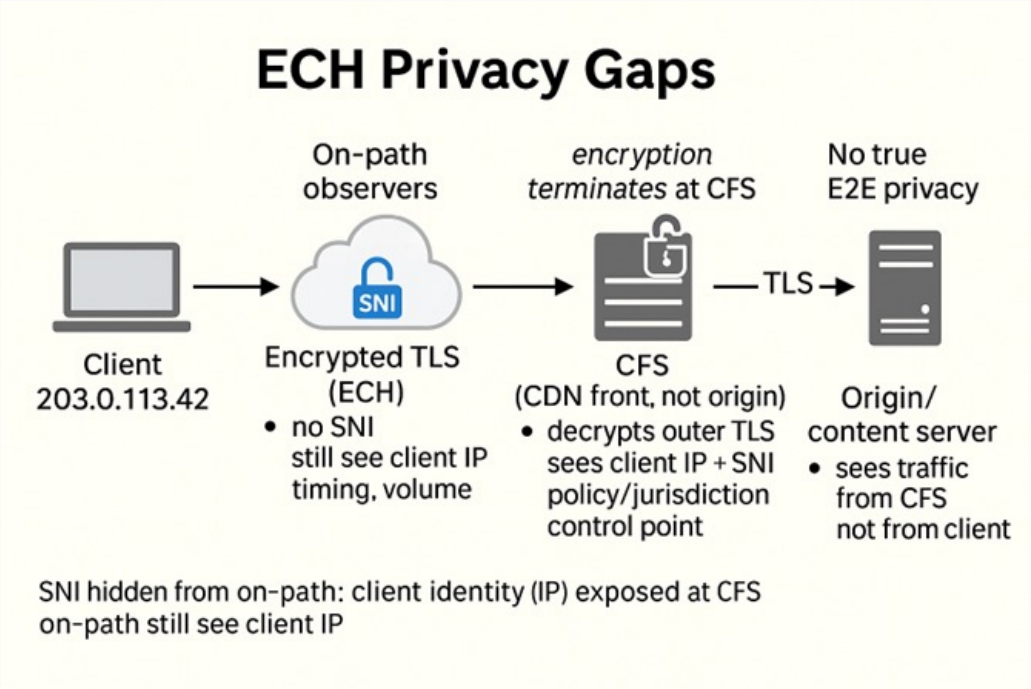
To provide destination privacy – protecting users against network-level tracking and censorship by encrypting TLS handshake metadata



Motivation – ECH Privacy Gaps

*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*

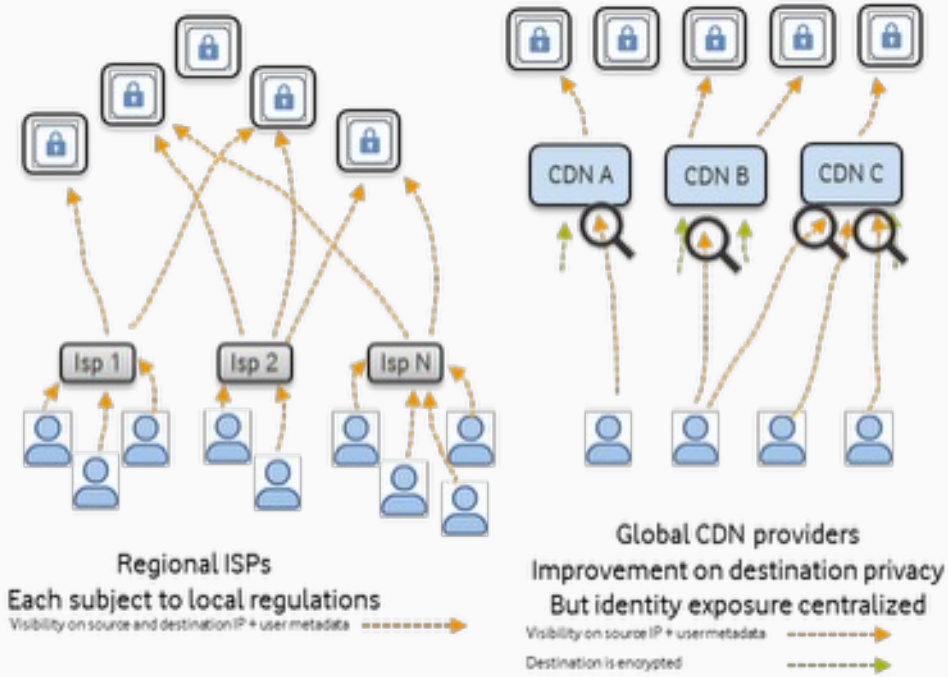


Motivation – ECH Centralization Gaps

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

risks:

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



Internet moves from decentralized to few control points

Architectural directions

Objective:
Explore architectural alternatives that preserve privacy and decentralization.

Transport-Level Privacy Enhancements:
- Use of ephemeral IPv6 source address pools (e.g., per-flow randomization).
- Coordinated address rotation via network-side mechanisms.

Relay-Based Decoupling:
- Lightweight relays (e.g., CFR) to mask source identity.
- Avoids full proxying or DNS involvement.

Endpoint Discovery Alternatives:
- Directory services or application-layer coordination.
- Endpoint based CFR selection

Customer-Facing Relay (CFR) proposal

Function:

- Decouples source IP from encrypted transport.
- Provides source ip randomization/rotation

Benefits:

- Preserves TLS/ECH semantics.
- Avoids DNS-layer complexity.

Deployment:

- ISP or enterprise edge.
- Compatible with CDN and non-CDN environments.

Question for DINRG

Feedback Needed:

- Is this direction aligned with DINRG's scope?
- Should DINRG initiate a focused effort or coordinate with other groups?

Next Steps:

- Draft refinement: draft-scalone-cfr-source-privacy-00
- Open to collaboration and refinement