DISPATCH
Internet-Draft
Intended status: Informational
Expires: 3 September 2026

G. Scalone
Vodafone

2 March 2026

Customer-Facing Relay (CFR): Enhancing Source Privacy in Encrypted Transport and CDN Scenarios

draft-scalone-cfr-source-privacy-01

Abstract

Encrypted Client Hello (ECH) improves destination privacy by encrypting the Server Name Indication in TLS, but the customer source identity-- typically the IP address and network metadata--remains observable to intermediaries such as CDNs, hosting providers, and recursive resolvers. This document introduces the _Customer-Facing Relay (CFR)_, a lightweight, transport-agnostic relay operated by access providers to decouple customer identity from encrypted destinations.
By forwarding opaque encrypted payloads (TCP or UDP) without terminating TLS or QUIC, a CFR complements ECH encryption to strengthen source privacy and reduce metadata correlation.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 3 September 2026.

Copyright Notice

Table of Contents

1. Introduction

While recent advances such as TLS 1.3 and ECH significantly improve destination privacy, they do not prevent intermediaries from observing the customer source identity. As content delivery infrastructures concentrate traffic, a small number of entities gain disproportionate visibility over user metadata.

The Customer-Facing Relay (CFR) architecture introduces a minimalistic relay positioned at the customers network edge to limit correlation. The CFR rewrites addressing metadata while forwarding encrypted traffic without termination, creating two semi-independent visibility domains: one for the access network (source) and one for the CDN or upstream service (destination). The result is improved source privacy and reduced metadata consolidation.

This document refines the CFR concept introduced in draft-00, elaborates the privacy model, and outlines potential discovery, deployment, and operational considerations.

2. Terminology

CFR: _Customer-Facing Relay_, A privacy-enhancing network function positioned at or near the access network. It rewrites source addresses while forwarding encrypted traffic without terminating TLS/QUIC.

CFS: _Client-Facing Server_ As defined in ECH (RFC 9460), the endpoint that terminates encrypted handshakes on behalf of origins. A CFR does not act as a CFS.

Upstream Service: _Upstream Service_ A CDN, hosting provider, or service endpoint that ultimately receives the relayed encrypted traffic.

Opaque Payload: _Opaque Payload_ Encrypted packets (TLS-over-TCP or QUIC-over-UDP) forwarded without modification.

3. Motivation

CDNs and major hosting platforms increasingly act as aggregation points for encrypted traffic. Even with ECH, these entities can link the customer source IP address to thousands of origins they serve. This centralization poses privacy and competition risks:

* Correlation risk: Access patterns across different encrypted services can be tied to a single user.

* Lack of architectural balance: Encryption protects destinations, but source privacy remains under-addressed.

* Cross-service tracking: Consolidated metadata enables pervasive behavioral observation.

CFRs seek to break the direct correlation between the customer and the encrypted destination by splitting visibility:

* Customer -> CFR -> CDN -> Origin

4. Customer-Facing Relay (CFR) Concept

A CFR is a deployable, narrow-function relay implemented by access networks, enterprises, or other operators. Its core behaviors include:

4.1. Characteristics

- *Transport-agnostic* - Works for both TCP and UDP encrypted traffic, forwarding opaque encrypted packets.
- *No TLS/QUIC termination* - Does not terminate or inspect TLS/QUIC; preserves end-to-end encryption.
- *Deployable* - Can be operated by access providers and enterprises.
- *Transparent* - Performs no content filtering, categorization, or inspection.
- *Discoverable* - May be discovered via DNS-based mechanisms such as DDR or DNR.
- *Lightweight operation* - Functions similarly to NAT, NAPT, or tunnel encapsulation, but for privacy purposes.
- *Policy-minimal* - Not intended for filtering, shaping, categorization, or interception

4.2. Privacy Model

Entity	Knows Source	Knows Destination	Content Visibility
Customer	X	X	X
CFR	X		
CDN		X	

Table 1

No single entity can link source and destination unless collusion or compromise occurs.

4.3. Deployment Models

- *ISP-embedded CFR* - Integrated in broadband or mobile access gateways.
- *Enterprise CFR* - For employee source privacy against cloud services.
- *Federated CFRs* - CFRs operated by third parties, potentially discoverable via DNS.

5. Relationship to Existing Work

- *ECH (RFC9460)* - Protects destination identity; CFR complements it by protecting source identity.

* *DPRIVE (DoH/DoT/DoQ)* - Encrypts DNS traffic; CFR addresses the transport-layer metadata.
* *PEARG / HRPC* - Explore broader issues of privacy and decentralization in Internet architecture.

6. Design Considerations and Open Questions

6.1. Discovery and Bootstrapping

* Use of DDR/DNR to advertise CFR endpoints.
* Trust establishment between customer devices and CFR operators.

6.2. Performance and Scalability

* Relay overhead and impact on latency.
* Stateless versus stateful design parameters.

7. Abuse Prevention

* Preventing use as an open relay.
* Integration with Privacy Pass or similar token-based systems.

8. Interoperability

* Potential chaining of multiple CFRs.
* Compatibility with QUIC migration and multipath mechanisms

9. IETF Standardization

* Target areas include DISPATCH, MASQUE, PEARG, or future CFR-specific working groups

10. Security Considerations

CFRs enhance privacy but introduce new risks:

* *Collusion risk* - If the CFR and CDN share data, correlation can be restored.
* *Abuse vectors* - Attackers could abuse CFRs for amplification or anonymization unless constrained.
* *Operational drift* - CFRs must not evolve into DPI or filtering points; specifications should explicitly prohibit modification or inspection.
* *Accountability tension* - Some deployments may need soft attribution mechanisms without compromising anonymity.
* *Need for IPv4/IPv6 NAT randomization standards* - CFR deployments rely on sourc address rewriting, but current NAT behaviors, especially for IPv6 prefix translation and IPv4 port allocation,

lack standardized, privacy preserving randomization requirements. A future standard should define deterministic entropy floors for address/port selection, avoid stable mappings, and ensure alignment with the CFR privacy model.

Further analysis is required to quantify threat models and formal privacy guarantees.

11. IANA Considerations

This document makes no IANA requests.

12. References

12.1. Informative References

* [RFC9460] Benjamin L. et al., _TLS Encrypted Client Hello_, RFC 9460, 2023.
* [RFC9325] Thomson, M., _Recommendations for Secure Use of TLS and DTLS_, RFC 9325, 2022.
* [I-D.ietf-add-ddr] _Discovery of Designated Resolvers (DDR)_, Internet-Draft, IETF ADD WG.
* [I-D.ietf-add-dnr] _Discovery of Network-designated Resolvers (DNR)_, Internet-Draft, IETF ADD WG.

13. Acknowledgments

The author acknowledges the helpful input and discussions from Andrew Campling, Arnaud Taddei, Kevin Smith, Lee Wilman, Tom Newton, and colleagues within Vodafone Group, DINRG, and DISPATCH.

Author’s Address

Gianpaolo Angelo Scalone
Vodafone