DISPATCH
Internet-Draft
Intended status: Informational
Expires: 23 April 2026

G. Scalone
Vodafone

20 October 2025

Customer-Facing Relay (CFR): Enhancing Source Privacy in Encrypted Transport and CDN Scenarios
draft-scalone-cfr-source-privacy-00

Abstract

Encrypted Client Hello (ECH) improves destination privacy by encrypting the Server Name Indication in TLS, but the customer’s 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 23 April 2026.

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology 2
3. Motivation 3
4. Customer-Facing Relay (CFR) Concept 3
5. Relationship to Existing Work 4
6. Open Questions 4
7. Security Considerations 4
8. IANA Considerations 5
9. References 5
9.1. Informative References 5
10. Acknowledgments 5
Author's Address 5

1. Introduction

While encryption technologies such as TLS 1.3 and Encrypted Client Hello (ECH) significantly enhance destination privacy, the source of connections remains exposed. Content delivery infrastructures can still observe customer IP addresses and associated metadata, enabling correlation of user behavior even when the content and destination name are protected.

This document proposes the _Customer-Facing Relay (CFR)_ architecture, which introduces a minimal intermediary between the customer and the encrypted destination to partition visibility of metadata. The intent is to complement existing privacy mechanisms by focusing on the source side of communication.

2. Terminology

CFR: _Customer-Facing Relay_, a privacy-enhancing network function located close to the end customer, for example within an ISP or enterprise access network.

CFS: _Client-Facing Server_ as defined in ECH. The CFS terminates encrypted handshakes on behalf of multiple origins. In contrast, the _CFR does not terminate TLS or QUIC sessions._ It forwards encrypted

packets while rewriting addressing information, similar to a NAT or tunnel endpoint, with the explicit goal of protecting customer source privacy.

3. Motivation

Destination privacy has improved through encryption, but this progress has increased traffic centralization. A small number of CDNs now terminate most encrypted sessions, consolidating visibility over user traffic. This creates an architectural imbalance: encryption hides _what_ is accessed but not _who_ is accessing it.

Observed effects:

* CDNs acting as Client-Facing Servers can correlate customer IPs across thousands of hosted domains.
* Aggregation of ECH traffic concentrates metadata in few entities.

CFRs aim to rebalance this asymmetry by separating customer identity from destination visibility.

4. Customer-Facing Relay (CFR) Concept

A Customer-Facing Relay (CFR) is a lightweight, privacy-oriented intermediary positioned at the customer’s network edge. It relays encrypted transport flows toward upstream services without decrypting or terminating them, rewriting source addressing to prevent direct correlation between the customer’s IP identity and the encrypted destination.

Customer ---> CFR ---> CDN ---> Origin Server

Characteristics:

* *Transport-agnostic* - Works for both TCP and UDP, forwarding opaque encrypted packets.
* *No TLS/QUIC termination* - The end-to-end encryption context is preserved.
* *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.

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

Table 1

By splitting knowledge between the CFR and the CDN, no single entity can fully correlate source and destination metadata.

Trust assumptions:

* The customer trusts the CFR not to expose source IP mappings.
* The CFR cannot read or modify encrypted traffic.
* The upstream service cannot identify the original customer.

5. Relationship to Existing Work

* *ECH (RFC9460)* - Protects destination identity; CFR complements it by protecting source identity.
* *MASQUE (CONNECT-UDP / CONNECT-IP)* - Provides tunnel mechanisms; CFR can reuse similar encapsulation but for privacy rather than proxying.
* *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. Open Questions

* How should CFR discovery and trust bootstrapping be achieved?
* What performance impacts arise from additional relay hops?
* Should CFRs support chaining or federation?
* How can abuse prevention coexist with privacy guarantees?
* Which IETF area or WG should progress standardization?

7. Security Considerations

CFRs enhance privacy by partitioning knowledge between multiple parties, but they also introduce new trust points and potential attack surfaces.

* *Collusion or compromise* - A malicious or compromised CFR could share mapping data with CDNs, restoring correlation. Transparency and operational independence are essential.
* *Inspection risk* - CFRs must not evolve into inspection or policy enforcement devices. The design goal is strict pass-through of opaque encrypted traffic.
* *Denial-of-Service* - CFRs could be abused as open relays or DoS amplifiers. Operators must implement rate limits, authentication, or Privacy Pass-like tokens.
* *Accountability vs. anonymity* - Further study is required to balance deployability with protection against abuse.

8. IANA Considerations

This document makes no IANA requests.

9. References

9.1. 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-masque-connect-udp] _The CONNECT-UDP Method for HTTP_, Internet-Draft, IETF MASQUE WG.
* [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.

10. 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