Network Working Group
Internet-Draft
Intended status: Informational
Expires: 10 July 2026

B.A. Fisher
DPA R&D

6 January 2026

The Universal Zero-Port Interconnect Framework (UZPIF): An Identity-Centric Architecture for Post-Port Networking
draft-dpa-uzpif-framework-00

Abstract

The Universal Zero-Port Interconnect Framework (UZPIF) describes a post-port networking model in which communication is established via outbound, identity-bound sessions to Rendezvous Nodes (RNs). By removing publicly reachable listening ports at endpoints, UZPIF aims to reduce exposure to Internet-wide scanning and unsolicited ingress, and to constrain a broad class of lateral-movement vectors.

This document outlines architectural motivation, a high-level security model, operational and economic considerations, a governance concept (Pantheon), and an incremental migration approach. UZPIF is intended to be read alongside companion work describing the Universal Zero-Port Transport Protocol (UZP; [UZP]) and TLS-UZP ([TLS-DPA]).

Table of Contents

1. Scope and Status

This document is an Internet-Draft and represents work in progress. It is published to enable structured technical review, interoperability discussion, and disciplined specification development around the Universal Zero-Port Interconnect Framework (UZPIF).

The material is a research artefact. It does not claim technical completeness, production readiness, or endorsement by the IETF or any other standards body, and it is not presented as a standards-track specification.

It is not a universal replacement, is not mandated outside its target environment, and is designed for experimentation and profile-driven deployments.

During conversion from internal research documents into IETF XML, care has been taken to:

* preserve a clear distinction between normative and informative content;

* use requirement language (e.g., "MUST", "SHOULD", "MAY") only where protocol behaviour is intentionally specified;

* avoid any implication of registry finalisation, mandatory implementation, or standard-track status; and

* maintain intellectual-property neutrality, with no implied patent grants or licensing commitments beyond the IETF Trust copyright licence applicable to Internet-Draft text.

Ongoing research, implementation, performance validation, and real-world pilot work remain outside the scope of this Internet-Draft text and may be pursued separately.

2. Executive Summary

The Internet still commonly exposes services via publicly reachable transport ports, a legacy design choice that enables scanning and unsolicited connection attempts at global scale. Operationally, this contributes to exposure for denial-of-service attacks, credential attacks, and lateral movement within networks.

UZPIF (the framework) and UZP ([UZP]) (its transport protocol) remove the concept of exposed ports at endpoints. Both endpoints initiate outbound, identity-anchored sessions to a Rendezvous Node (RN), which only stitches traffic when identity, context, and declared purpose align under policy issued by Pantheon, the identity and policy plane.

The intent is a model where nothing is discoverable unless explicitly permitted by policy and exposed through the rendezvous fabric, and where application traffic is end-to-end authenticated and encrypted. UZP ([UZP]) is designed to support performance properties such as:

* block-level reliability,

* selective retransmission, and

* deterministic pacing.

Legacy applications (e.g., HTTP(S), remote desktop, file sharing, and real-time media) are intended to continue to operate without modification via a Host Identity Layer (HIL) that maps traditional application expectations onto identity-centric sessions.

UZPIF is intended to be evolutionary rather than revolutionary. It deliberately builds on transport, security, and identity work embodied in QUIC [RFC9000], TLS 1.3 [RFC8446], and the Host Identity Protocol [RFC7401], while aligning with modern zero-trust guidance (e.g., NIST SP 800-207 [NIST-SP800-207]) and post-quantum cryptography standardisation efforts (e.g., the NIST PQC project [NIST-PQC]).

3. Introduction

This document provides an architectural overview of UZPIF and motivates why an identity-first, rendezvous-based model that avoids publicly reachable listeners may be desirable.

3.1. Why Now?

* Investment in perimeter defences (e.g., DDoS mitigation and application firewalls) can yield diminishing returns as attackers automate scanning and exploit discovery at Internet scale.

* Zero Trust Network Access (ZTNA) and SASE deployments indicate demand for identity-first networking, yet many approaches still expose TCP/UDP ingress and rely on perimeter constructs. [NIST-SP800-207]

* Post-quantum cryptography efforts provide a path to identity-first transport without prohibitive performance regression as key encapsulation and signature schemes mature. [NIST-PQC]

3.2. What’s New Versus Yet Another VPN?

Conventional VPNs and overlay networks typically retain the assumption that services listen on IP:port tuples, even if those ports are only reachable within a private address space or through a gateway. QUIC [RFC9000], TLS 1.3 [RFC8446], HIP [RFC7401], and systems such as Tor [Tor] demonstrate that identity, encryption, and rendezvous can be decoupled from raw addressing semantics, but they

stop short of removing listening ports entirely.

* *No listeners* at endpoints.

* *Identity-as-address* via identities (e.g., canonical and ephemeral identities) rather than IP:port.

* *Block-level reliability* with selective retransmission (transport-level design goal).

* *Pantheon policy plane* encoding purpose, context, and validity into every session.

4. Terminology

Requirements Language: The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] and [RFC8174] when, and only when, they appear in all capitals.

This Internet-Draft is primarily architectural; requirement language is used sparingly and only where behaviour is intentionally specified.

EP Endpoint. A host or service that participates in UZPIF by initiating outbound sessions.

RN Rendezvous Node. A mediator that accepts outbound sessions and stitches permitted flows.

Pantheon An identity, attestation, and policy plane that issues credentials and session grants.

HIL Host Identity Layer. A compatibility layer intended to support legacy applications over identity-centric sessions.

CID Canonical Identity. A long-term cryptographic identity used to identify an EP (or a delegated sub-identity).

EID Ephemeral Identity. A short-lived identity used for sessions, derived or issued under policy.

ZPIT Zero-Port Interconnect Tunnel. An end-to-end encrypted tunnel stitched via one or more RNs.

5. Core Architecture

5.1. High-Level Flow: EP to RN to EP

In UZPIF, both peers initiate outbound sessions towards an RN. After policy evaluation and authorisation, the RN stitches the two sessions into a tunnel (ZPIT) that carries end-to-end protected application data.

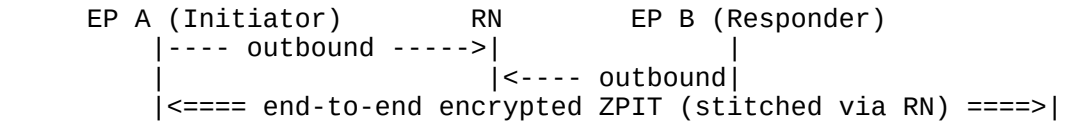

Figure 1: High-level communication pattern (outbound-only sessions)

This figure shows both endpoints initiating outbound sessions to the RN, which stitches them into a single ZPIT.

5.2. Pantheon Grant Verification

Prior to stitching, an EP is expected to obtain a signed authorisation ("Grant") from Pantheon. Grants bind identity to purpose and validity constraints, enabling RNs to make consistent policy decisions.

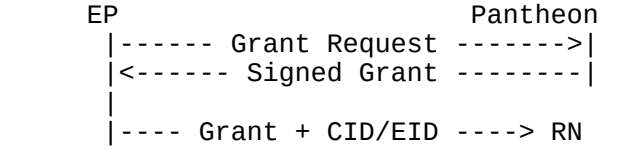

Figure 2: Grant request and issuance flow

This figure illustrates the basic grant request and issuance exchange between an EP and Pantheon.

5.3. Flow Stitching by the RN

The RN establishes a stitched tunnel only if both peers present acceptable identities and authorisations. The RN is assumed to be able to drop, delay, or reorder packets, but is not expected to learn end-to-end protected application plaintext.

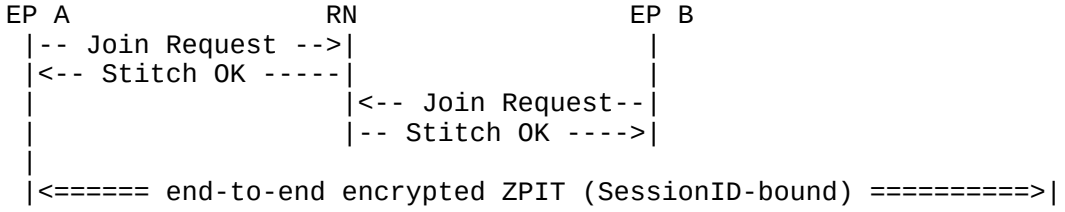

Figure 3: Join and stitch establishment

This figure shows the RN joining two authorised sessions into a stitched tunnel without learning plaintext.

5.4. Multi-RN Stitching for High-Assurance Tenants

UZPIF can be extended to multi-hop stitching, for example where a tenant requires multiple independently operated RNs and attestation chains. End-to-end protection is expected to remain between endpoints.

EP A -> RN1 -> RN2 -> EP B

EP A <======== end-to-end AEAD protected traffic ========> EP B

Figure 4: Multi-hop stitching with end-to-end authenticated encryption

This figure depicts a multi-hop RN chain while end-to-end AEAD protection remains between endpoints.

6. Pantheon: Identity and Governance Model

Pantheon is described here as a global identity, attestation, and policy plane. This section sketches the model at a conceptual level; future revisions may refine data structures and operational assumptions.

6.1. Identity Model

Pantheon issues (or authorises issuance of):

* long-term signing keys (forming CIDs);
* ephemeral session keys (forming EIDs); and
* delegated sub-identities for services or microprocesses.

This identity approach is conceptually aligned with HIP’s separation of endpoint identities from locators [RFC7401], but elevated to a policy plane.

6.2. Certificate Format

Pantheon Certificates (PCerts) may include the following conceptual elements:

* a CID and public signing key (and optionally a post-quantum key encapsulation key);
* purpose tags (e.g., service, role, tenant);
* validity bounds (time or epoch); and
* optional attestation claims (e.g., hardware trust or enclave measurement).

6.3. Grant Structure

A Grant is described as a signed assertion binding:

* the CID/EID of the requester;
* the requested peer identity;
* purpose and action;
* a time window and replay nonce; and
* an authorised quality-of-service (QoS) class.

6.4. Attestation Model

RNs and endpoints may publish attestations such as:

* hardware and software measurements;
* configuration hashes; and
* policy compliance data.

Pantheon is expected to store these in transparency logs, mirroring transparency and verifiability goals in broader zero-trust guidance. [NIST-SP800-207]

6.5. Caching Rules

Endpoints may cache:

* PCerts for 24 hours;

* Grants for the shorter of their validity window or session lifetime; and

* attestation proofs for the duration of RN handshake paths.

7. Benefits and Trade-offs

UZPIF and UZP ([UZP]) intentionally reuse established transport and cryptographic primitives, but change where and how they are bound to identity, policy, and reachability. In particular, QUIC [RFC9000] and TLS 1.3 [RFC8446] demonstrate encrypted transports with modern handshake properties, while UZPIF shifts the reachability model away from listening endpoints.

Dimension	UZPIF/UZP ([UZP])	Traditional TCP/TLS	QUIC/TLS
Exposure	No open ports (endpoints are not publicly listening)	Open ports and/or proxies	Open ports at network edge
Identity	Mandatory cryptographic identity	Typically TLS-level identity only	TLS-level identity
Reliability	Block-level (design goal)	Segment-level	Stream-level
RN trust	Drop/delay only (no end-to-end plaintext visibility expected)	N/A	N/A
Latency control	Deterministic pacing (design goal)	Congestion control variants (e.g., Reno/ CUBIC)	Congestion control variants (e.g., BBR/ CUBIC)
Legacy applications	Supported via HIL (intended)	Native	Often requires gateways or adaptation
Post-quantum readiness	Designed for cryptographic agility	Inconsistent deployment	Emerging

Table 1: Comparison of transport architectures

8. Threat Model

This section sketches attacker classes and example controls. It is not a complete security analysis and will evolve with implementation experience.

Attacker classes include:

* Internet-wide scanners;

* botnets seeking command-and-control beacons;

* malicious RNs (assumed capable of drop/delay/reorder);

* insiders with credentials; and

* traffic analysts performing correlation.

Existing rendezvous and overlay systems (e.g., Tor [Tor]) and NAT traversal mechanisms based on STUN [RFC5389] and TURN [RFC5766] demonstrate the power of indirection, but they still assume exposed or discoverable listeners somewhere in the path. UZPIF's design intent is to remove those listeners from the endpoint security model.

Example controls discussed for UZPIF include:

* end-to-end authenticated encryption (AEAD);

* RN and endpoint attestation;

* puzzles and identity-bound rate limits;

* multi-RN stitching for higher assurance; and

* post-quantum readiness and cryptographic agility (see [NIST-PQC]).

9. Economics

* Capital expenditure reduction: reduced reliance on perimeter appliances and complex DMZ designs.

* Operational expenditure reduction: fewer ACL/NAT rule changes and less inbound exposure management.

* Risk reduction: reduced externally visible attack surface.

* Potential service models: governance and RN validation as managed components.

10. Migration Plan for Organisations

UZPIF is intended for incremental deployment alongside existing TCP/TLS and QUIC-based stacks [RFC8446] and [RFC9000].

1. *Deploy an RN:* Introduce an outbound-only rendezvous node.

2. *Deploy the HIL:* Install the Host Identity Layer on endpoints.

3. *Dual-stack operation:* Run UZP ([UZP]) alongside existing TCP/TLS.

4. *Cutover:* Migrate services gradually to zero-port operation.

11. Security Considerations

UZPIF's central security claim is that avoiding publicly reachable listeners at endpoints reduces exposure to scanning and unsolicited ingress. However, the framework introduces reliance on identity, authorisation, and policy evaluation components (e.g., Pantheon and RNs) whose compromise or misconfiguration could impact availability and authorisation correctness.

The threat model in Section 8 discusses attacker classes and candidate controls. Future revisions of this document (and the companion UZP ([UZP]) and TLS-UZP ([TLS-DPA]) documents) are expected to provide a more systematic analysis, including key management, revocation, attestation trust, and traffic analysis resistance.

12. IANA Considerations

This document has no IANA actions.

UZPIF is an architectural framework and does not define protocol parameters requiring registries.

13. References

13.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

13.2. Informative References

[NIST-PQC] National Institute of Standards and Technology, "NIST Post-Quantum Cryptography Standardization Project", 2022, <https://csrc.nist.gov/Projects/post-quantum-cryptography>.

[NIST-SP800-207]
Rose, S., Borchert, O., Mitchell, S., and S. Connelly, "Zero Trust Architecture", NIST SP 800-207, 2019, <https://doi.org/10.6028/NIST.SP.800-207>.

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, DOI 10.17487/RFC5389, October 2008, <https://www.rfc-editor.org/info/rfc5389>.

[RFC5766] Mahy, R., Matthews, P., and J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", RFC 5766, DOI 10.17487/RFC5766, April 2010, <https://www.rfc-editor.org/info/rfc5766>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/info/rfc7401>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/info/rfc9000>.

[TLS-DPA] Fisher, B. A., "TLS-DPA: An Identity-Bound Security Protocol for Traditional, Overlay, and Zero-Port Transports", Work in Progress, Internet-Draft, draft-dpa-tls-dpa, <https://datatracker.ietf.org/doc/html/draft-dpa-tls-dpa>.

[Tor] Dingledine, R., Mathewson, N., and P. Syverson, "Tor: The Second-Generation Onion Router", 2004, <https://www.usenix.org/legacy/publications/library/proceedings/sec04/tech/full_papers/dingledine/dingledine.pdf>.

[UZP] Fisher, B. A., "UZP: Universal Zero-Port Transport Protocol", Work in Progress, Internet-Draft, draft-dpa-uzp-transport, <https://datatracker.ietf.org/doc/html/draft-dpa-uzp-transport>.

Appendix A. Appendix A: Technical Specification (Excerpt)

A.1. Abstract

UZP ([UZP]) defines an identity-addressed, encrypted-by-default transport protocol for zero-port networking. Endpoints do not listen on IP/port tuples; both create outbound sessions to an RN.

A.2. Terminology

* EP - endpoint.
* RN - rendezvous node.
* Pantheon - identity/policy authority.
* HIL - Host Identity Layer.
* CID - canonical identity.
* EID - ephemeral identity.
* ZPIT - stitched tunnel.
* Block - reliability unit.
* Frame - payload unit.

A.3. Architectural Overview

1. EP opens a control channel to an RN.
2. EP authenticates with Pantheon.
3. EP requests a Join for a peer CID.
4. RN validates authorisation and stitches a ZPIT.
5. Data flows with deterministic pacing (transport design goal).

Author’s Address

Benjamin Anthony Fisher
DPA R&D Ltd (https://www.dpa-cloud.co.uk)
Email: b.fisher@dpa-cloud.co.uk
URI: https://orcid.org/0009-0004-4412-2269