Network Working Group
Internet-Draft
Intended status: Informational
Expires: 6 July 2026

B.A. Fisher
DPA R&D Ltd (https://www.dpa-cloud.co.uk)

2 January 2026

UZP: Universal Zero-Port Transport Protocol
draft-dpa-uzp-transport-00

Abstract

The Universal Zero-Port Transport Protocol (UZP) defines an identity-addressed, encrypted-by-default transport for the Universal Zero-Port Interconnect Framework (UZPIF; [UZPIF]). Instead of exposing IP:port listeners, both endpoints establish outbound, identity-bound sessions to one or more Rendezvous Nodes (RNs). The RN performs flow stitching but never terminates end-to-end cryptography or holds long-term secrets. All application data is carried over an authenticated encryption (AEAD) channel keyed by a handshake based on modern and post-quantum-capable primitives. Reliability is expressed at the block level, rather than at the TCP segment or stream level, enabling selective retransmission and deterministic pacing. This document specifies the UZP wire format, handshake, cryptographic negotiation, exporter interface, 0-RTT rules, replay model, and RN behaviour, and its relationship to UZPIF ([UZPIF]), QUIC ([RFC9000]), HIP ([RFC7401]), and TLS 1.3 ([RFC8446]).

Note to Reviewers

This document is an Internet-Draft derived from internal research material solely to enable structured technical review, interoperability discussion, and disciplined specification development under the Internet-Draft process. It is a work-in-progress research artefact and does not constitute a standard, recommendation, or finished specification.

The text aims to preserve a clear separation of normative and informative content. Requirement words are used only where protocol behaviour is intentionally specified. Where this document provides numeric guidance (for example timers, windows, or congestion-related tuning), the intent is to offer recommended bounds suitable for experimentation; profile-based behaviour and implementation discretion are explicitly expected within stated limits.

UZP is designed for identity-first, zero-port environments where conventional port-based transport assumptions do not hold; it is not presented as a universal replacement for existing transports.

Status of This Memo

Copyright Notice

Table of Contents

1. Scope and Status

This Internet-Draft describes UZP as an experimental transport protocol for the Universal Zero-Port Interconnect Framework (UZPIF; [UZPIF]). The intent is to support early peer review and implementation experiments; substantial revision is expected.

Unless otherwise stated, design parameters and numeric values are provided as numeric guidance and recommended bounds, rather than as fixed constants. Implementations may adopt alternative congestion tuning, profile-based behaviour, and implementation-defined choices within the constraints explicitly described in the relevant sections.

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

2. Introduction

The deployed Internet largely continues to rely on listening sockets bound to IP:port tuples. This design, inherited from the 1980s, exposes every reachable service to scanning, unsolicited ingress, and a wide class of lateral-movement and amplification attacks. Contemporary defences such as WAFs, DDoS scrubbing, layered ACLs, and micro-segmentation treat the symptom, not the cause.

The Universal Zero-Port Interconnect Framework (UZPIF; [UZPIF]) proposes a post-port architecture in which services are reached only via outbound, identity-bound connections to Rendezvous Nodes (RNs). UZP is the transport protocol that operates beneath UZPIF ([UZPIF]) and is designed for identity-first, zero-port environments where conventional port-listening assumptions do not hold. In that context, it provides transport and security semantics comparable to conventional TCP+TLS or QUIC+TLS data planes, while keeping legacy applications unmodified above a Host Identity Layer (HIL).

The design builds on ideas from QUIC [RFC9000], HIP [RFC7401], and Zero Trust Architecture [NIST-SP800-207]. Rendezvous-based systems such as Tor [TOR2004] demonstrate the value of decoupling endpoint identity from network location. UZP is intended to be compatible with post-quantum cryptography profiles [NIST-PQC].

2.1. Conventions and Terminology

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, as shown here.

This document uses terminology from UZPIF ([UZPIF]) and related work:

* Endpoint (EP): A host participating in UZP communication. EPs never listen on public IP:port tuples.

* Rendezvous Node (RN): A relay node that accepts outbound connections from EPs, validates Pantheon-issued Grants, and stitches identity-bound flows.

* Pantheon: The global identity, attestation, and policy plane used by UZPIF ([UZPIF]) and UZP.

* Canonical Identity (CID): A long-lived, cryptographic identifier derived from a principal’s public signing key.

* Ephemeral Identity (EID): A per-session identity bound to short-lived key material.

* Block: The unit of reliability (acknowledgement / retransmission) in UZP.

* Frame: The unit of application payload mapping inside a block.

3. Design Goals

UZP is intended to satisfy the following primary goals:

* Zero exposed ports: EPs MUST operate with no listening sockets reachable from the public Internet. All communication originates from outbound connections to RNs.

* Identity-first addressing: The fundamental addressing object is a cryptographic identity (CID/EID), not an IP:port pair, following the spirit of HIP [RFC7401].

* Encrypted-by-default: All application data MUST be carried over an AEAD-protected channel, with forward secrecy and exporter support comparable to TLS 1.3 [RFC8446].

* Modern and PQ-capable: The handshake MUST support both classical and post-quantum key exchange and authentication, with algorithm agility and central policy control [NIST-PQC].

* Block-level reliability: Reliability is expressed at the block level, enabling selective retransmission and deterministic pacing similar in spirit to, but distinct from, QUIC's stream framing [RFC9000].

* RN minimal trust: RNs MUST NOT learn application plaintext or hold long-term identity secrets; they may only drop, reorder, or delay encrypted traffic.

Where this document provides numeric guidance (for example, congestion-related tuning, replay windows, or pacing), it is intended as recommended bounds for experimentation. Implementations may apply profile-based behaviour and implementation-defined tuning within any explicit limits stated in the relevant sections.

4. Architectural Overview

At a high level, UZP operates as follows:

1. Each EP opens one or more outbound control channels to one or more RNs.

2. The EP authenticates to Pantheon and obtains Grants that authorise communication with a peer identity under specific policy.

3. To talk to another EP, the initiator submits a Join request to an RN, containing its own CID/EID, the target CID, and the relevant Grant material.

4. The responder independently connects to an RN (which MAY be the same RN or a different RN in the same trust domain) and presents its own Grants.

5. The RN stitches the two UZP sessions into a zero-port interconnect tunnel (ZPIT) once both sides have been validated.

The RN never terminates end-to-end cryptography; each side performs a UZP handshake with the RN, derives end-to-end keys using exporter material, and then switches to E2E AEAD for application data.

4.1. High-Level Session Flow

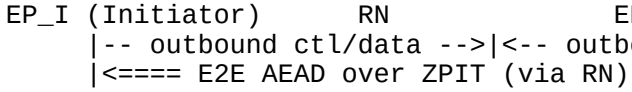

Figure 1: High-level communication pattern: both endpoints initiate outbound- only connections to the RN, which stitches an end-to-end ZPIT.

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

4.2. Identity Model and CID Stability

Pantheon issues long-term signing keys to principals; the canonical identity CID is defined as a hash (e.g., BLAKE3) of the public signing key. CIDs are intended to be stable over multi-year time scales and across multiple devices in the same administrative entity, and SHOULD only change when the underlying key is rotated or revoked due to compromise.

Each transport session also has an Ephemeral Identity (EID), derived from short-lived key material. EIDs are bound to CIDs via Pantheon-issued credentials and are used within the UZP handshake and record layer.

This separation mirrors the long-term vs. ephemeral key split in both HIP [RFC7401] and TLS 1.3 [RFC8446].

5. Handshake Overview

The UZP handshake provides:

* Mutual (or unilateral) authentication bound to CIDs and EIDs.
* Negotiation of cipher suites and AEAD algorithms.
* Derivation of exporter keys for UZPIF ([UZPIF]) and higher layers.
* Integration of Pantheon Grants, including replay protection and policy binding.

The RN forwards handshake messages but does not terminate the cryptographic handshake itself. Instead, both EPs derive end-to-end secrets using exporter material bound to the identities and Grants, and then switch to direct AEAD protection across the ZPIT.

5.1. Flight Diagram

Figure Figure 2 sketches a representative two-party handshake mediated by an RN. Exact messages and encoding are defined in the wire-format section (not reproduced in full here).

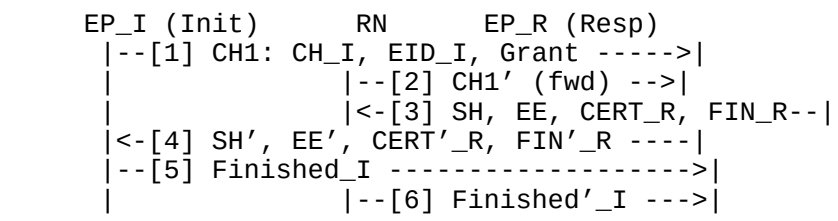

Figure 2: Example UZP handshake flights via an RN. Message indices [1]-[6] are explained in the legend. Labels are illustrative; exact message contents are defined in the wire specification.

This figure summarizes the RN-relayed handshake flights and where forwarding occurs.

Legend:

[1] CH1: ClientHello_I, EID_I, Grant

[2] CH1': Forwarded ClientHello_I

[3] SH, EE, CERT_R, FIN_R

[4] SH', EE', CERT'_R, FIN'_R

[5] Finished_I (initiator final confirm towards RN)

[6] Finished'_I (forwarded initiator confirm towards responder)

6. Cryptographic Negotiation and AEAD Tag Length

UZP supports an extensible cipher-suite registry. A cipher suite includes:

* A key exchange mechanism (e.g., X25519, or a PQ KEM candidate).

* A signature algorithm for authentication.

* An AEAD algorithm for record protection (e.g., AES-GCM-128, ChaCha20-Poly1305).

* A KDF (e.g., HKDF-SHA256 or a BLAKE3-based KDF).

6.1. AEAD Tag Length

The AEAD tag length is algorithm-dependent but subject to the following constraints:

* Implementations MUST use a tag length of at least 96 bits for all UZP application data records.

* When an AEAD algorithm allows variable tag lengths, endpoints SHOULD use the algorithm’s full tag length (typically 128 bits for AES-GCM) and MUST NOT negotiate a tag length below 96 bits.

* The tag length used for a session is fixed for the lifetime of that session and is implied by the negotiated cipher suite.

This requirement follows common practice in modern protocols, which treat 96 bits as a practical lower bound on AEAD authentication tags for wide-area deployments, while allowing future AEADs with different native tag lengths.

7. Blocks, Frames, and Reliability

UZP uses a block-oriented reliability model:

* A block is a unit of transmission and acknowledgement.

* Each block contains one or more frames, which carry application data or control information.

* Blocks carry monotonically increasing block numbers, and ACK frames reference blocks, not individual bytes.

This block-level model enables selective retransmission and deterministic pacing:

* EPs can rapidly detect loss patterns and retransmit only affected blocks.

* Congestion control and pacing can be applied over well-defined block units, similarly to how QUIC applies logic over packet and frame boundaries [RFC9000].

Blocks are encrypted and authenticated with the negotiated AEAD. The associated data includes:

* CID and EID for both parties.

* Direction and block number.

* A context-specific label (e.g., "uzp-application" or "uzp-handshake").

8. Exporters

UZP defines an exporter interface analogous to TLS exporters [RFC8446]. Exporters derive context-specific keys from the main handshake secrets, using labels and context values that MUST be bound to identities and transport parameters.

An exporter input consists of:

* A label (e.g., "uzpif-zpit-key").

* A context value (which may include CIDs, EIDs, RN identifiers, and Grant nonces).

* An output length.

Exported keys are used by:

* UZPIF ([UZPIF]) to derive per-ZPIT keys for monitoring or additional encapsulation.

* Higher-layer protocols wishing to bind application security directly to UZP session properties.

Exporters MUST incorporate both CIDs and the negotiated transport parameters so that re-use of exporters across sessions is cryptographically separated.

9. 0-RTT Data and Replay Handling

UZP allows, but tightly constrains, 0-RTT (early) data:

* Early data MAY be sent by a client that possesses a valid, non-expired session resumption token and a Pantheon Grant that explicitly permits early data.

* Early data MUST be cryptographically distinct from 1-RTT data and MUST be bound to a monotonically increasing Grant nonce.

* RNs MUST treat 0-RTT flows as replayable at the transport level and MUST NOT rely on transport-layer properties for replay prevention.

Replay prevention is handled jointly by:

* Pantheon Grants, which include a Grant nonce and time window; replayed Grants outside their window MUST be rejected.

* Endpoints, which track nonces and session tickets, and MUST refuse to process 0-RTT requests that would not be safe to replay at the application level.

If Pantheon policy specifies "no-replay" for a given Grant, endpoints MUST NOT use 0-RTT for any traffic under that Grant, and RNs MUST drop any early data tagged with that policy.

10. Post-Quantum Profiles and Crypto Agility

Given the long-term horizon of identity-centric networking, UZP is designed to support post-quantum (PQ) algorithms:

* Cipher suites define both classical and PQ-capable KEMs and signature schemes.

* Pantheon policy can enforce that certain tenants or epochs require PQ-only or hybrid key exchange.

* The handshake format allows negotiation of PQ suites in parallel with classical ones, similar to ongoing PQ-TLS efforts [NIST-PQC].

Transport endpoints SHOULD support at least one PQ KEM and one PQ-capable signature algorithm as they become standardised.

11. Rendezvous Node Behaviour

RNs are designed to be minimally trusted intermediaries. An RN:

* Accepts outbound connections from EPs and validates their Pantheon-issued credentials and Grants.

* Matches Join requests between EPs and stitches them into ZPITs according to policy.

* Relays encrypted blocks between stitched endpoints, potentially applying rate limits, traffic shaping, and policy enforcement on encrypted metadata.

Importantly, an RN:

* MUST NOT terminate end-to-end UZP AEAD protection.

* MUST NOT hold long-term secrets for EP identities.

* MAY observe and act on limited metadata (e.g., CIDs, block counts, timing) comparable to the exposure in QUIC's on-path model [RFC9000].

For high-assurance deployments, multi-RN topologies similar to onion routing may be used [TOR2004], with attestation chains that prove that each RN conforms to specified software and configuration baselines.

12. Security Considerations

UZP's security properties derive from:

* The zero-port architecture of UZPIF ([UZPIF]) (no open listeners).

* The use of modern AEAD algorithms with at least 96-bit tags.

* Identity-first addressing via CIDs and EIDs, influenced by HIP [RFC7401].

* Exporters that bind higher-layer security directly to transport identities and parameters.

* Strong replay controls via Grants and endpoint tracking of nonces and tickets.

Residual risks include traffic analysis, RN compromise (drop/delay behaviour), and application-layer weaknesses. These are mitigated through:

* Multi-RN topologies and attestation.

* Pantheon policy that can revoke identities and Grants quickly.

* Integration with Zero Trust principles [NIST-SP800-207].

13. IANA Considerations

This document makes no requests of IANA at this time. Future revisions of UZP may define registries for protocol parameters (for example cipher suites, frame types, and exporter labels), but such actions are out of scope for this introductory specification.

* A registry for UZP cipher suites and AEAD algorithms.

* A registry for frame and block types.

* A registry for exporter labels used by UZP and UZPIF ([UZPIF]).

14. 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>.

15. Informative References

[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>.

[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>.

[UZPIF] Fisher, B. A., "Universal Zero-Port Interconnect Framework (UZPIF)", Work in Progress, Internet-Draft, draft-dpa-uzpif-framework, <https://datatracker.ietf.org/doc/html/draft-dpa-uzpif-framework>.

[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>.

[NIST-PQC] Technology, N. I. O. S. A., "NIST Post-Quantum Cryptography Standardization: Fourth Round Candidate Algorithms", 2022, <https://csrc.nist.gov/Projects/post-quantum-cryptography>.

[TOR2004] Dingledine, R., Mathewson, N., and P. Syverson, "Tor: The Second-Generation Onion Router", USENIX Security Symposium, 2004.

Acknowledgements

The author thanks colleagues and early reviewers for discussions on identity-centric networking, rendezvous transports, and post-quantum transition considerations. Any errors or omissions remain the author’s responsibility.

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