Independent Submission
Internet-Draft
Intended status: Informational
Expires: December 6, 2026

C. Hopley
AlgoVoi

June 4, 2026

Post-Quantum Credential Binding for x402 Agentic Payment Authorization
draft-hopley-x402-pqc-credential-binding-00

Abstract

This document defines how Falcon-1024 (NIST FIPS 206 / FN-DSA) and ML-DSA-65 (NIST FIPS 204) credentials bind to x402 agentic payment authorization. It specifies the credential envelope format, the JCS canonicalization discipline applied to signed payloads, the gateway verification procedure, and the session token binding that replaces per-request API key authentication for credentialed agents.

This is the first Internet-Draft in the agentic payments space to anchor credential binding to the NIST post-quantum cryptography standards (FIPS 203/204/206).

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 December 6, 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

1.

The x402 payment protocol {{x402}} enables HTTP-native micropayments between autonomous agents and API providers. As agent deployments scale, two problems emerge:

This document addresses both by defining a credential binding scheme where:

1.1.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174].

An entity that evaluates an agent and signs a credential asserting the result. The reference implementation is the AlgoVoi Agent Trust Bench.

The x402 payment gateway that accepts credentials and issues session tokens.

An autonomous software system presenting credentials to a gateway in exchange for payment-authorization session tokens.

A Falcon-1024-signed credential asserting that an agent passed adversarial evaluation. Phase 1 contains a plaintext score; Phase 2 replaces the score with a Bulletproofs range proof (zero-knowledge).

2.

A PQC credential is a JSON object serialised to UTF-8 and encoded as base64url (without padding). The structure is:

2.1.

MUST be one of:

The

algorithm is the RECOMMENDED choice. It provides 1,024-bit classical security, 256-bit post-quantum security, and compact signatures (~1,280 bytes).

2.2.

A 16-character lowercase hex string derived as:

The gateway MUST verify that the

in the envelope matches the

of the issuer’s public key in its trusted-key registry before proceeding to signature verification.

2.3.

A JSON object. Required fields for ATB Phase 2 credentials:

The

field MUST decode to exactly 32 bytes (a compressed Ristretto255 point). The

field MUST decode to 200-900 bytes (a 64-bit Bulletproofs range proof over Ristretto255).

2.4.

Base64url-encoded detached signature over the JCS-canonical form of the

field. The signer applies RFC 8785 {{RFC8785}} canonicalization to the

object, then signs the resulting UTF-8 bytes.

For

, the signature is a Falcon-1024 detached signature (NIST FIPS 206, PQClean format, ~1,280 bytes, base64url).

3.

The issuer:

The issuer MUST NOT include the

field in the payload before signing. The

and

envelope fields MUST NOT be signed.

4.

The gateway receiving

:

A gateway SHOULD implement an LRU cache keyed by

to avoid re-running Falcon verification for repeated presentations within the cache TTL. The cache TTL MUST NOT exceed the credential’s

.

5.

On successful credential verification, the gateway issues a session token:

Response:

The session token is a JWT {{RFC7519}} signed with the gateway’s HMAC key. Its claims include

,

,

(in micro-USD),

, and

. Subsequent requests carry only:

No API key or tenant header is required for the session duration.

5.1.

The gateway tracks cumulative spend per

in-process. On each successful payment,

is incremented. If

, the gateway MUST reject the request with HTTP 402.

6.

Implementations SHOULD prefer Falcon-1024 for its signature compactness in HTTP header contexts.

7.

7.1.

An adversary with a cryptographically-relevant quantum computer can break Ed25519 and ES256 signatures using Shor’s algorithm. All credentials using these algorithms are vulnerable to retrospective forgery once such a machine exists. Issuers SHOULD migrate to Falcon-1024 or ML-DSA-65 before quantum computers reach this capability threshold.

7.2.

Phase 2 ATB credentials include a Bulletproofs range proof rather than a plaintext score. The range proof attests that

without revealing the exact score. Gateways MUST NOT attempt to reconstruct scores from commitment values.

7.3.

The

in each session token is a random 128-bit value generated at issuance. Gateways MUST track issued

values and reject replayed tokens. The credential

in Phase 1 activation flows prevents replay at the license-activation layer.

7.4.

Issuers SHOULD rotate Falcon-1024 keys at least annually. The

field allows gateways to maintain a key registry and identify credentials by key version without revoking the full issuer DID.

8.

This document has no IANA actions.

Appendix A.

A.1.

A.2.

Author’s Address

Christopher Hopley
AlgoVoi

Email: hello@algovoi.co.uk