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

C. Hopley
AlgoVoi

June 4, 2026

Cross-Issuer ZKP Federation for Post-Quantum Agentic Payment Credentials
draft-hopley-x402-federation-zkp-00

Abstract

This document defines a protocol for composing independently-issued post-quantum ZKP credentials from different issuers into a single federation token, without requiring a shared trust root between issuers.

Each credential is a Falcon-1024 (NIST FIPS 206) or ML-DSA-65 (NIST FIPS 204) signed Bulletproofs range proof asserting that an agent’s trust score meets a threshold. A federation validator independently verifies each credential against its issuer’s public key, then computes a composite commitment binding all verified proofs.

The resulting federation token is signed by the validator alone. No issuer needs to know about the others. This solves the cross-issuer attestation composition problem in agentic payment networks.

1.

1.1.

Agentic payment networks are converging on a multi-issuer credential landscape. An agent may hold credentials from:

A gateway that requires proof of compliance with N issuers faces a composition problem: how does it accept a single credential that proves all N conditions are met, without requiring:

The naive solution -- accept N separate credentials and verify each -- works but has two drawbacks:

This document specifies a federation composition protocol that:

1.2.

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 signs PQC credentials (ATB hub, identity provider, etc.). Each issuer has an independent Falcon-1024 or ML-DSA-65 key pair. Issuers have no knowledge of each other.

An entity that holds the public keys of N trusted issuers and composes their credentials into a single federation token. The validator may be the payment gateway itself, or a separate service trusted by the gateway.

A short-lived HMAC-SHA256-signed token produced by the federation validator, containing the composite commitment and issuer list.

A SHA-256 hash binding the Pedersen commitments from all N input credentials together with a per-composition nonce.

2.

The agent presents two or more PQC credentials (each from an independent issuer) to the federation validator. The validator verifies each, composes the commitments, and returns a federation token. The agent then uses this token on the gateway.

The gateway only needs to: 1. Verify the HMAC on the federation token. 2. Verify expiry. 3. Check spend cap.

No Falcon-1024 verification happens on the gateway hot path.

3.

Each credential presented to the federation validator MUST conform to {{CREDENTIALBINDING}} S.2 (ATB Phase 2,

).

Specifically: -

MUST be

or

. -

MUST decode to exactly 32 bytes (compressed Ristretto255). -

MUST decode to 200-900 bytes (64-bit Bulletproofs range proof). -

MUST be a DID present in the validator’s

registry. - The credential MUST not be expired.

The validator MUST independently verify each credential’s Falcon-1024 signature before proceeding to composition.

4.

The federation validator maintains a mapping:

Each issuer’s public key is obtained from their

endpoint:

The validator MUST NOT accept credentials from issuers not in its registry. This is the sole trust boundary: the validator trusts specific issuer keys, but issuers do not need to trust each other.

5.

5.1.

5.2.

For each credential

, extract the Pedersen commitment:

Sample a per-composition nonce:

Compute the composite commitment:

where:

The domain label provides separation from other SHA-256 uses. The nonce ensures the composite commitment is unique per composition event, preventing an adversary from reusing a subset of credentials with different partners to produce a matching composite.

5.3.

The federation token’s

MUST be set to:

This ensures the federation token never outlives any of its input credentials.

5.4.

The validator constructs the following payload:

Applies JCS canonicalization {{RFC8785}} to produce

.

Computes the HMAC tag:

Assembles the federation token envelope:

Base64url-encodes the envelope JSON as the federation token string.

6.

The gateway receiving

(after the initial session exchange):

The gateway does NOT re-verify Falcon-1024 signatures on the hot path. That work was done once by the federation validator.

7.

7.1.

Issuers A and B have independent key pairs. The validator's only relationship to each issuer is possession of their public keys. Issuers do not need to communicate with each other or with the validator beyond publishing their public keys.

7.2.

Each credential in the composition is independently verifiable by any party holding the issuer's public key. The composite token does not obscure this: the

field in the token payload lists all issuers and their kids, allowing retrospective audit.

7.3.

The composite commitment

binds the federation token to the exact set of Pedersen commitments from the input credentials. An adversary who replaces one credential with a different one will produce a different

and the HMAC will not verify.

The per-composition nonce prevents a partial-credential-set replay: an adversary cannot use commitment_A from one composition event and commitment_B from another to produce a valid composite.

7.4.

The ZKP range proof in each input credential asserts

without revealing the exact score. The composite commitment is derived from Pedersen commitment bytes, not from scores. The gateway learns only that

.

7.5.

All per-credential signing uses Falcon-1024 (NIST FIPS 206) or ML-DSA-65 (NIST FIPS 204). The composite token uses HMAC-SHA256, which is quantum- resistant under the birthday-bound model (Grover's algorithm reduces effective security from 256 to 128 bits -- still adequate).

7.6.

If the validator's HMAC key is compromised, an adversary can forge federation tokens. Operators SHOULD rotate the validator key regularly and revoke outstanding tokens on rotation by advancing the token's

.

8.

8.1.

An HMAC-based federation token is verifiable by any instance holding the validator secret. In multi-instance deployments the secret MUST be shared across instances (e.g. via a secrets manager), not per-instance.

8.2.

Operators SHOULD configure

to require cross-issuer evidence. A value of 1 provides single-issuer mode -- useful for testing but does not demonstrate cross-issuer composition.

8.3.

The protocol permits two credentials from the same issuer. The composite commitment is still computed correctly and the HMAC verifies. However, the "no shared trust root" property holds trivially in this case. Operators that require distinct issuers SHOULD enforce issuer-DID uniqueness in the validator configuration.

8.4.

Full Bulletproofs range proof verification (step 10 of {{CREDENTIALBINDING}} S.4) requires calling the ATB ZKP service. The federation validator package performs structural validation of proof fields without the Rust service. Operators requiring cryptographic range proof verification SHOULD configure

and the

environment variable.

9.

The composition pattern in this document is novel in the agentic payments context. It draws on:

10.

This document has no IANA actions.

Appendix A.

A.1.

A.2.

Author’s Address

Christopher Hopley
AlgoVoi

Email: hello@algovoi.co.uk