Independent Submission
Internet-Draft
Intended status: Informational
Expires: 26 November 2026

V. Research
Vauban Research

25 May 2026

Post-Quantum Cryptographic Discipline for x402 STARK Receipts
draft-vauban-x402-pqc-receipts-01

Abstract

This document specifies a post-quantum cryptographic discipline for x402 STARK receipts. The discipline applies on two layers : (a) proof integrity via hash-based proving systems (the Stwo Circle STARK M31 reference implementation), which are post-quantum sound under standard cryptanalytic assumptions, and (b) signature integrity via the hybrid ES256K + ML-DSA-65 dual-signed receipt variant ([FIPS204]). It maps the hybrid-pqc receipt variant of the x402 STARK Receipt Format Extension ([STARK-RECEIPTS]) to the NIST PQC migration roadmap and to the EU eIDAS 2.0, ANSSI, and BSI migration timelines for the 2025-2030 window. Reference runners are published as the vauban-x402-jcs-conformance and vauban-x402-canonical Rust crates. Companion documents are [STARK-RECEIPTS] (receipt format) and [VPSF-ALGEBRA] (composability grammar).

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 26 November 2026.

Copyright Notice

Table of Contents

1. Introduction

Classical payment receipts signed under elliptic-curve schemes such as ES256K become forgeable under a sufficiently capable quantum adversary. The base x402 PAYMENT-RESPONSE ([X402-V2]) uses ES256K as its default signature scheme. Under the present specification, a PAYMENT-RESPONSE retained for audit purposes in year N is verifiable today, but its long-term integrity depends on the absence of a quantum computer capable of executing Shor's algorithm against secp256k1. NIST timelines ([NIST-PQC-MIGRATION]), ANSSI guidance ([ANSSI-PQC]), and BSI guidance ([BSI-PQC]) converge on a 2030-2035 horizon for the migration of high-value or long-retention cryptographic material away from classical-only signatures.

This document defines a two-axis post-quantum cryptographic discipline for x402 receipts that addresses the long-term integrity gap. The first axis applies at the proof-system layer : the stark-vauban-pay-v1 variant of [STARK-RECEIPTS] uses Stwo Circle STARK M31 ([STWO]), a hash-based proving system whose soundness rests on the collision and second-preimage resistance of cryptographic hash functions rather than on algebraic hardness assumptions broken by Shor's algorithm. The second axis applies at the signature layer : the hybrid-pqc variant of [STARK-RECEIPTS] composes ES256K and ML-DSA-65 ([FIPS204]) signatures over the identical JCS canonical preimage, producing a receipt that remains verifiable if either single algorithm is broken.

This document positions the discipline as the recommended profile for x402 deployments that operate under statutory retention obligations (for example, MiCA Art. 80 or EU AI Act Art. 12 transparency-and-documentation duties). The discipline does not modify the wire format defined in [STARK-RECEIPTS] or the composability grammar defined in [VPSF-ALGEBRA] ; it constrains the choice of cryptographic primitives and the negotiation discipline that producers and verifiers SHOULD apply to satisfy post-quantum soundness for the 2025-2030 migration window and beyond.

This document is an Independent Submission. It is not the product of an IETF Working Group. It is published for community review and to establish a stable reference for implementors.

2. 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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.1. Terminology

Post-Quantum Sound: A cryptographic construction whose security holds against an adversary in possession of a large-scale quantum computer (specifically, an adversary capable of executing Shor’s algorithm against discrete logarithm and integer factorisation problems, and Grover’s algorithm against unstructured search). A construction is post-quantum sound if no known quantum algorithm reduces its security below an operationally acceptable level. SHA-256, as used in hash-based proving systems, is post-quantum sound at 128-bit security under Grover (which provides at most a quadratic speedup against generic preimage search).

Hash-Based Proof System: A succinct proof system whose soundness reduces to the collision and second-preimage resistance of an underlying cryptographic hash function rather than to algebraic assumptions (pairings, discrete logarithms, factorisation). STARK proof systems are hash-based. SNARK proof systems based on pairings (BN254, BLS12-381) are not hash-based.

ML-DSA: Module-Lattice-Based Digital Signature Algorithm, standardised in [FIPS204]. This document references the ML-DSA-65 parameter set, which provides 192-bit classical security and an estimated 128-bit security against quantum adversaries per NIST’s category-3 classification.

Hybrid Signature: A composite signature scheme that produces two or more independent signatures over the same canonical message under disjoint cryptographic assumptions. A hybrid signature is valid if and only if every component signature verifies independently. The hybrid construction is secure against an adversary that breaks any proper subset of the component schemes.

Migration Window: The temporal interval between the publication of post-quantum standards (NIST FIPS 204, August 2024) and the deprecation of classical-only signatures under applicable regulatory frameworks. For this document, the migration window spans 2025 to 2030, with deprecation horizons varying by jurisdiction.

Backwards Compatibility: The property that a receipt produced under this discipline is verifiable by an implementation that supports only classical primitives, provided the classical component of the receipt is well-formed and independently verifiable. The hybrid receipt variant satisfies backwards compatibility ; the STARK proof system at the proof layer is independent of signature backwards compatibility.

3. Threat Model : Quantum Adversary

3.1. Assumed Capability

The threat model assumes an adversary in possession of a large-scale, fault-tolerant quantum computer capable of executing Shor’s algorithm against classical public-key primitives and Grover’s algorithm against unstructured search problems. The timeline for the availability of such a machine is uncertain ; NIST guidance ([NIST-PQC-MIGRATION]) and ANSSI guidance ([ANSSI-PQC]) recommend migration planning for high-value or long-retention cryptographic material on a 2030-2035 horizon, with concrete migration steps starting in 2025.

The adversary is assumed to have :

* Access to public-key material (signature verification keys) for all receipts ever published.

* The ability to record receipts in transit and at rest indefinitely (the "harvest-now-decrypt-later" assumption).

* No access to private signing material held by facilitators ; key compromise is treated separately in Section 8.

3.2. Receipt Forgery Vectors

Three forgery vectors are relevant for x402 receipts under the quantum threat model :

3.2.1. ES256K Signature Break

ES256K signatures are based on the discrete logarithm problem over the secp256k1 elliptic curve. Shor's algorithm reduces the discrete logarithm problem to polynomial time on a quantum computer. An adversary with a sufficiently large quantum computer can recover the private signing key from the public verification key, and thereafter forge arbitrary receipts under the compromised key. This vector affects every receipt signed under ES256K, retroactively, once the adversary's quantum capability becomes available.

3.2.2. Hash Collision Under Grover

The JCS canonical preimage discipline ([RFC8785]) and the receipt content addressing in [STARK-RECEIPTS] both rely on SHA-256. Grover's algorithm provides at most a quadratic speedup against unstructured search, reducing the effective security of a 256-bit hash output from 128 bits classical to 128 bits quantum against second-preimage attack. SHA-256 therefore remains post-quantum sound at the 128-bit security level for the use cases of this document (preimage chaining and content addressing). No mitigation is required at the hash layer for the receipt formats specified in [STARK-RECEIPTS].

3.2.3. Algebraic Proof System Soundness Break

SNARK proof systems whose soundness rests on bilinear pairings (BN254, BLS12-381, or equivalent) are vulnerable to Shor's algorithm in the same manner as ES256K : the underlying discrete-logarithm hardness assumption is broken. A SNARK-based receipt becomes forgeable once the adversary can recover trapdoor material from the proving key. This vector does not affect STARK proof systems, which rely only on hash-function security.

3.3. Out-of-Scope Threats

The following threats are out of scope for this document :

* Key encapsulation mechanism analysis ; ML-KEM ([FIPS203]) is treated in the NIST guidance but does not apply to receipt signature integrity.

* Quantum-secure channel establishment (TLS, x402 transport layer) ; this document concerns receipt integrity at rest, not transport.

* Side-channel attacks against signing implementations ; see Section 8 for hardening guidance specific to constant-time ML-DSA-65 implementations.

4. Two-Axis PQC Discipline

The post-quantum cryptographic discipline for x402 STARK receipts operates on two orthogonal layers. A deployment selects one or both axes based on its threat model and regulatory environment.

4.1. Proof System Layer

4.1.1. Hash-Based Proving Requirement

The proof system underlying a receipt variant MUST be hash-based for the variant to be considered post-quantum sound at the proof layer. The stark-vauban-pay-v1 variant of [STARK-RECEIPTS] satisfies this requirement by using the Stwo Circle STARK M31 prover ([STWO]). Stwo Circle STARKs construct succinct proofs from Merkle commitments and a hash-based polynomial-IOP transformation ; the soundness reduction relies on the collision and second-preimage resistance of the underlying hash function (Blake2s in the Stwo reference implementation), neither of which is broken by Shor’s algorithm.

4.1.2. Forbidden Proof System Families

Implementations claiming post-quantum soundness at the proof layer MUST NOT use any of the following proof system families :

* Groth16, PLONK, or any SNARK construction based on bilinear pairings over BN254, BLS12-381, or equivalent curves.

* Bulletproofs or any range proof construction whose soundness reduces to the discrete logarithm problem.

* Any proof system whose security analysis explicitly invokes the algebraic group model or generic group model without additional hash-based safeguards.

A facilitator that advertises a stark-vauban-pay-v1-tier receipt MUST in fact use a hash-based proof system. A facilitator that internally uses a pairing-based SNARK and labels the result as a STARK receipt is in violation of this discipline and MUST NOT claim conformance.

4.2. Signature Layer

4.2.1. Hybrid Composition Requirement

A receipt variant that claims post-quantum soundness at the signature layer MUST carry two independent signatures over the identical JCS canonical preimage ([RFC8785]) : one classical signature (ES256K) and one post-quantum signature (ML-DSA-65 per [FIPS204]). The hybrid-pqc variant of [STARK-RECEIPTS] satisfies this requirement.

A verifier processing a hybrid-pqc receipt MUST :

1. Confirm that both signature (ES256K) and pqc_signature (ML-DSA-65) cover the byte-identical JCS canonical preimage.

2. Verify each signature independently against the corresponding public key referenced by kid_es256k and kid_mldsa65.

3. Reject the receipt if either signature fails to verify. A receipt with a valid ES256K signature and an invalid ML-DSA-65 signature MUST be rejected under the hybrid discipline ; partial verification is not equivalent to verification.

4.2.2. Classical Fallback Discipline

The classical-es256k variant of [STARK-RECEIPTS] carries only an ES256K signature and is NOT post-quantum sound at the signature layer. Deployments operating under statutory retention obligations SHOULD treat the classical-es256k variant as a legacy interop format only, and SHOULD migrate to hybrid-pqc or stark-vauban-pay-v1 before the relevant deprecation horizon. The classical fallback remains valid for non-retention deployments where the threat model permits.

4.2.3. Migration Window Profile

During the 2025-2030 migration window, the recommended profile is :

* For deployments under statutory retention obligations : hybrid-pqc REQUIRED ; classical-es256k rejected for new receipts ; existing classical-es256k receipts re-stamped as hybrid-pqc on first re-presentation to a supervisor (re-stamping mechanism is implementation-specific and out of scope here).

* For deployments without statutory retention obligations : hybrid-pqc RECOMMENDED ; classical-es256k ACCEPTED for interop with non-PQ-ready counterparties.

Post-2030, classical-only signature variants SHOULD be deprecated for new receipt issuance. The exact deprecation date is jurisdiction-dependent and SHOULD follow the applicable NIST, ANSSI, BSI, or eIDAS guidance.

5. Receipt Format Mapping

The two-axis discipline defined in this document maps to the receipt variants of [STARK-RECEIPTS] as follows.

5.1. Proof System Layer Mapping

Variant	Proof system	Post-quantum sound at proof layer?
stark-vauban-pay-v1	Stwo Circle STARK M31 (hash-based)	Yes
hybrid-pqc	None (signature-only variant)	Not applicable
classical-es256k	None (signature-only variant)	Not applicable

Table 1

5.2. Signature Layer Mapping

Variant	Signature scheme	Post-quantum sound at signature layer?
stark-vauban-pay-v1	Facilitator-specific outer signature	Implementation-dependent
hybrid-pqc	ES256K + ML-DSA-65 (hybrid)	Yes
classical-es256k	ES256K only	No

Table 2

The two layers are orthogonal. A stark-vauban-pay-v1 receipt provides proof-layer post-quantum soundness ; if the deployment also requires signature-layer post-quantum soundness for the outer

signature, it SHOULD combine the STARK proof with a hybrid signature in the same receipt envelope. This combination is permitted by [STARK-RECEIPTS] provided both the proof and the hybrid signature cover the identical canonical preimage.

5.3. PQ-Readiness Negotiation

The receipt-format negotiation defined in [STARK-RECEIPTS] is the carrier for PQ-readiness signalling. A facilitator advertising post-quantum soundness MUST list hybrid-pqc or stark-vauban-pay-v1 (or both) in the X-Payment-Options header. A client requiring post-quantum soundness MUST include receipt_format with required: true in the PAYMENT-SIGNATURE extension, naming the required variant.

A facilitator that lists hybrid-pqc in X-Payment-Options but cannot in fact produce a valid ML-DSA-65 signature is in protocol violation. Conformance testing for PQ-readiness SHOULD include emission of a hybrid-pqc receipt and independent verification of both component signatures by a third-party verifier.

6. NIST PQC Migration Alignment

6.1. NIST Migration Roadmap

The post-quantum cryptography migration roadmap published by NIST ([NIST-PQC-MIGRATION]) defines a multi-stage transition from classical public-key primitives to standardised post-quantum primitives. Key milestones relevant to x402 receipt integrity :

* August 2024 : publication of [FIPS204] (ML-DSA), [FIPS203] (ML-KEM), and FIPS 205 (SLH-DSA). Implementations may begin production deployment.

* 2025 : recommended start of hybrid deployment for high-value or long-retention systems.

* 2030-2035 : recommended completion of migration ; classical-only systems SHOULD be deprecated for new deployments.

The hybrid-pqc variant of [STARK-RECEIPTS] aligns with the NIST hybrid deployment recommendation. The stark-vauban-pay-v1 variant addresses the proof-system layer in parallel and is independent of the signature migration timeline.

6.2. EU and Member State Alignment

The EU eIDAS 2.0 regulation ([EIDAS-2]) introduces requirements for qualified electronic signature schemes that anticipate the post-quantum transition. National guidance documents from ANSSI ([ANSSI-PQC]) and BSI ([BSI-PQC]) publish concrete migration timelines for cryptographic primitives used in regulated sectors.

A facilitator operating in an EU jurisdiction SHOULD :

* Publish a migration plan for ES256K to ML-DSA-65 (or a successor scheme endorsed by the applicable national authority) aligned with the relevant jurisdictional timeline.

* Issue hybrid-pqc receipts as the default variant for any payment context subject to long-term retention (MiCA Art. 80, AMLR Art. 56, DORA Art. 14, or sector-specific obligations).

* Document the post-quantum readiness of its receipt infrastructure in its qualified-trust-service-provider attestations where applicable.

6.3. NIST SP 800-208 Hybrid Composition Guidance

NIST [SP800-208] provides hybrid composition guidance for hash-based signature schemes. While SP 800-208 focuses on stateful hash-based signatures (LMS, XMSS), the composition principles for hybrid construction are relevant to the hybrid-pqc variant of [STARK-RECEIPTS]. Implementations SHOULD :

* Compose the two component signatures over the identical canonical message, not over a transformed version of the message.

* Treat the hybrid signature as a single object for serialisation purposes, with both component signatures present in every well-formed receipt.

* Reject any receipt where one of the two component signatures is absent, malformed, or fails verification.

The composition pattern in the hybrid-pqc variant follows these principles.

7. Implementation Evidence

7.1. Hash-Based Proof System Reference

The Stwo Circle STARK M31 prover ([STWO]) is the reference implementation of a hash-based proof system suitable for the stark-vauban-pay-v1 variant of [STARK-RECEIPTS]. The prover has been operationally deployed on Starknet mainnet since 2025 and is the proving substrate for the reference deployment documented in [STARK-RECEIPTS] (Sepolia demo at demo.pay.vauban.tech).

The Vauban Pay reference adapter for Stwo Circle STARK M31 is published as an Apache 2.0 Rust crate within the Vauban zkpay workspace. The adapter exposes a chain-agnostic proof backend interface ; the hash-based property of the underlying proof system is preserved across adapter implementations.

7.2. JCS Preimage Discipline Reference

The JCS canonical preimage discipline used by all three receipt variants is implemented in the vauban-x402-jcs-conformance Rust crate ([VAUBAN-JCS-CRATE]). The crate provides conformance vectors and a runner that has been cross-validated byte-identical against four other independent JCS implementations (Python, TypeScript, Go, Java) as documented in [STARK-RECEIPTS].

The canonical Claim Algebra encoder used to construct the preimage objects covered by the hybrid signature is implemented in the vauban-x402-canonical crate ([VAUBAN-CANONICAL-CRATE]). Both crates are published under Apache 2.0 on crates.io.

7.3. ML-DSA-65 Implementation Status

Production-quality ML-DSA-65 implementations exist in the open-source cryptographic library ecosystem (notably pq-crystals/dilithium and oqs-rust). At the time of publication of this document, a dedicated Vauban Pay crate wrapping ML-DSA-65 for the hybrid-pqc receipt variant is planned for delivery in Phase 2 of the Vauban Pay roadmap. Until then, implementations of the hybrid-pqc variant relying on third-party ML-DSA-65 crates remain conformant provided the crate implements [FIPS204] faithfully.

The third-party FeedOracle hybrid-PQC reference implementation listed in [STARK-RECEIPTS] (Axis 2 fixture set [X402-2411]) is the operational reference for the hybrid-pqc variant.

8. Security Considerations

8.1. Implementation Downgrade Attack

An adversary in a network position between the client and the facilitator MAY attempt to strip hybrid-pqc from the X-Payment-Options header, forcing the client to fall back to classical-es256k. The resulting receipt is not post-quantum sound, leaving the long-term integrity exposed.

Mitigation : a client requiring post-quantum soundness MUST send receipt_format with required: true in PAYMENT-SIGNATURE extensions, naming the required variant. A facilitator that cannot honour the request MUST return HTTP 402 with UnsupportedReceiptFormat rather than silently downgrading. Verifiers SHOULD cross-check the X-Receipt-Format header on the PAYMENT-RESPONSE against the client’s required variant and reject mismatches.

8.2. Insecure Hybrid Composition

A naive hybrid signature implementation that signs different canonical messages with the two component schemes does not provide the intended security property : an adversary who breaks ES256K can produce a forged classical signature, and the verifier may accept the receipt if the verification logic treats the two signatures as covering disjoint content.

Mitigation : implementations MUST follow the composition principles described in Section 6.3 : both signatures MUST cover the byte-identical JCS canonical preimage. The reference encoder in [VAUBAN-CANONICAL-CRATE] produces a single canonical byte string consumed by both signing operations.

8.3. ML-DSA-65 Side-Channel Exposure

ML-DSA-65 signing operations involve rejection sampling, secret-dependent control flow, and floating-point or arithmetic operations whose timing may leak secret-key material to a co-located adversary. Side-channel analysis of lattice-based signatures is an active research area.

Mitigation : ML-DSA-65 signing implementations used in production facilitator infrastructure MUST be constant-time and MUST be hardened against the classes of side-channel attack documented in the implementation’s threat model. Implementors SHOULD select ML-DSA-65 libraries that have undergone public side-channel analysis (for example, libraries audited by the post-quantum cryptography community since the publication of [FIPS204]).

8.4. STARK Proof System Auditability

The post-quantum soundness claim for STARK proof systems relies on the collision and second-preimage resistance of the underlying hash function. A flaw in the prover-verifier implementation, or in the polynomial-IOP transformation, may produce false-positive verifications independent of the hash function’s strength.

Mitigation : implementations SHOULD use a reference STARK prover that has undergone public audit ; the Stwo prover ([STWO]) is the reference for this document. Implementations that fork or modify the reference prover SHOULD re-audit the modifications against the original soundness analysis before production deployment.

8.5. Migration Timing Risk

Premature deprecation of classical signature support may exclude legitimate counterparties that have not yet migrated to post-quantum infrastructure. Conversely, late migration leaves long-retention receipts exposed to retroactive forgery once a quantum adversary becomes available.

Mitigation : deployments SHOULD align their deprecation schedule with the applicable jurisdictional guidance ([NIST-PQC-MIGRATION], [ANSSI-PQC], [BSI-PQC], [EIDAS-2]). The 2025-2030 hybrid deployment window described in Section 4.2.3 provides a five-year overlap during which both classical and post-quantum verification paths SHOULD be supported. Facilitators operating in regulated sectors SHOULD publish their migration plan in advance of any deprecation step affecting external counterparties.

9. IANA Considerations

This document has no IANA actions. It defers to the x402 Receipt Format registry established in [STARK-RECEIPTS] for the registration of the hybrid-pqc and stark-vauban-pay-v1 tokens that the discipline specified in this document maps onto. Future extensions introducing additional post-quantum receipt variants SHOULD register the corresponding tokens in that registry and reference this document for migration profile alignment.

Acknowledgments

The author thanks the participants in the x402 Linux Foundation coalition for the shared canonicalisation discipline and the hybrid-PQC receipt fixture set contributions documented in [STARK-RECEIPTS] and [X402-2411]. The author thanks the NIST Post-Quantum Cryptography working group for the standardisation of [FIPS204], [FIPS203], and the migration guidance referenced throughout this document. The author thanks the StarkWare Industries team for the publication of the Stwo Circle STARK M31 prover ([STWO]) as an open-source reference for hash-based proving systems.

Known Adopters and Reference Implementations

This appendix documents reference implementations and adopters of this specification confirmed at the time of publication. The list is informational and will be updated in subsequent revisions as additional implementations are reported.

Primary Maintainer

Vauban Pay (https://pay.vauban.tech) maintains the reference post-quantum receipt specification, the published conformance vectors (https://github.com/vauban-org/x402-stark-receipts-conformance), and the reference implementations listed below. The PQC discipline integrates ML-DSA-65 (NIST FIPS 204) for hybrid signatures and the Stwo Circle STARK M31 prover ([STWO]) for hash-based receipt integrity.

Reference Implementation Matrix

The conformance vector suite maintains an 8-implementation reference matrix across Python, JavaScript, Go, Java, Rust, PHP, Ruby, and C#. The first five are validated byte-for-byte against upstream JCS RFC 8785 libraries ; the last three are published as pure-stdlib reference runners pending CI execution. Detailed validation status is documented in _attestations/2026-05-25-vauban-8-impl-extended.md in the conformance vectors repository.

The published Vauban Pay packages across 3 ecosystems : vauban-x402-jcs-conformance@0.1.0, vauban-x402-canonical@0.1.0, vauban-x402-wire@0.1.0 on crates.io (including the vauban-x402-pqc-signer crate skeleton for ML-DSA-65 signature integration) ; vauban-x402-stark-receipt@0.1.0 on PyPI ; @vauban-pay/substrate@0.1.0 on npm.

Adoption Process

Implementers SHOULD notify the IETF contact at research@vauban.tech when adopting this specification in production. Adoption notifications include the post-quantum signature scheme implemented (FIPS 204 ML-DSA parameter set, hybrid mode if applicable), the STARK prover and hash function configuration, the canonical preimage discipline emitted, and the contact for follow-on coordination. Reported adopters will be listed in the next revision of this appendix following a verification step against the conformance vector matrix.

References

Normative References

[FIPS204] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard (ML-DSA)", August 2024, <https://doi.org/10.6028/NIST.FIPS.204>.

[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/rfc/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/rfc/rfc8174>.

[RFC8785] Rundgren, A., Jordan, B., and S. Erdtman, "JSON Canonicalization Scheme (JCS)", RFC 8785, DOI 10.17487/RFC8785, June 2020, <https://www.rfc-editor.org/rfc/rfc8785>.

[SP800-208] National Institute of Standards and Technology, "Recommendation for Stateful Hash-Based Signature Schemes", October 2020, <https://doi.org/10.6028/NIST.SP.800-208>.

[STARK-RECEIPTS] "x402 STARK Receipt Format Extension", Work in Progress, Internet-Draft, draft-vauban-x402-stark-receipts-01, n.d., <https://datatracker.ietf.org/doc/draft-vauban-x402-stark-receipts/>.

[VPSF-ALGEBRA]
"VPSF Claim Algebra for x402 Payment Receipts", Work in Progress, Internet-Draft, draft-vauban-x402-vpsf-algebra-00, n.d., <https://datatracker.ietf.org/doc/draft-vauban-x402-vpsf-algebra/>.

Informative References

[ANSSI-PQC]
Agence nationale de la securite des systemes d’information, "ANSSI Position Paper on Post-Quantum Cryptography Migration", n.d., <https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography>.

[BSI-PQC] Bundesamt fur Sicherheit in der Informationstechnik, "BSI Technical Guideline TR-02102 (cryptographic mechanisms)", n.d., <https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html>.

[EIDAS-2] European Parliament and Council, "Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 (eIDAS 2.0)", April 2024, <https://eur-lex.europa.eu/eli/reg/2024/1183/oj>.

[FIPS203] National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)", August 2024, <https://doi.org/10.6028/NIST.FIPS.203>.

[NIST-PQC-MIGRATION]
National Institute of Standards and Technology, "Post-Quantum Cryptography Migration Roadmap", n.d., <https://csrc.nist.gov/projects/post-quantum-cryptography>.

[STWO] "Stwo Circle STARK Prover (StarkWare Industries)", n.d., <https://github.com/starkware-libs/stwo>.

[VAUBAN-CANONICAL-CRATE]
"vauban-x402-canonical: canonical Claim Algebra encoder", n.d., <https://crates.io/crates/vauban-x402-canonical>.

[VAUBAN-JCS-CRATE]
"vauban-x402-jcs-conformance: JCS preimage discipline reference runner", n.d., <https://crates.io/crates/vauban-x402-jcs-conformance>.

[X402-2411]
"Hybrid-PQC receipt-core fixture set (Axis 2)", n.d., <https://github.com/x402-foundation/x402/pull/2411>.

[X402-V2] "x402 Linux Foundation V2 Working Group", n.d., <https://github.com/x402-foundation/x402>.

Appendix A. References

A.1. Normative References

(Normative references are listed in the document header.)

A.2. Informative References

(Informative references are listed in the document header.)

Author’s Address

Vauban Research
Vauban Research
Email: research@vauban.tech
URI: https://pay.vauban.tech