FIX Extension Pack Gap Analysis:
Cryptographic Audit Trail for Algorithmic Trading

Document ID: VSO-GAP-FIX-001 | **Version:** 1.0 | **Date:** 2025-12-22 | **Status:** Public Discussion

Executive Summary

This gap analysis identifies missing FIX Protocol capabilities for **cryptographically verifiable audit trails** in algorithmic trading. EU AI Act Article 12 and MiFID II RTS 25 require logging capabilities that current FIX messages cannot fully address.

1. Regulatory Requirements

Regulation	Requirement	FIX Support
EU AI Act Art. 12	Automatic logging with traceability	■ Partial
MiFID II RTS 25	Clock sync ≤100µs, audit trails	■ Partial
MiFID II RTS 6	Algo identification & testing	■ EP292/EP297
SEC Rule 17a-4	Tamper-evident records	■ Not addressed
IOSCO AI Guidance	Explainability, audit evidence	■ Not addressed

2. Identified Gaps

Gap 1: Clock Synchronization Evidence

FIX timestamps (Tag 52, 60) capture time but not synchronization quality. Regulators cannot verify RTS 25 clock sync compliance.

Proposed Tag	Name	Values
20004	ClockSyncStatus	0=Unknown, 1=NTP, 2=PTP, 3=GPS, 4=Atomic
20006	TimestampPrecision	0=Second, 1=Millisecond, 2=Microsecond, 3=Nanosecond

User-defined range (20001-20999) for PoC. Formal tag allocation via FIX GTC if adopted as EP.

Gap 2: Cryptographic Integrity Chain

No mechanism to prove log completeness or detect tampering. Messages are independent with no chain linking.

Proposed Tag	Name	Description
20001	AuditEventHash	SHA-256 hash of message content
20002	AuditPrevHash	Hash of previous message in chain
20005	AuditMerkleRoot	Periodic batch anchor for efficient verification

Gap 3: AI Decision Audit Trail

EP292/EP297 provide algo identification but do not standardize a portable representation of decision evidence.

Proposed Tag	Name	Description
20007	AlgoDecisionFactors	JSON array of factor names
20008	AlgoConfidenceScore	0.0-1.0 decision confidence
20009	AlgoExplainMethod	SHAP, LIME, rule-based, etc.

Designed to extend, not replace, existing EP292/EP297 fields.

Gap 4: Non-Repudiation and Evidence Records

Current FIX audit relies on submitter's integrity with no independent verification mechanism.

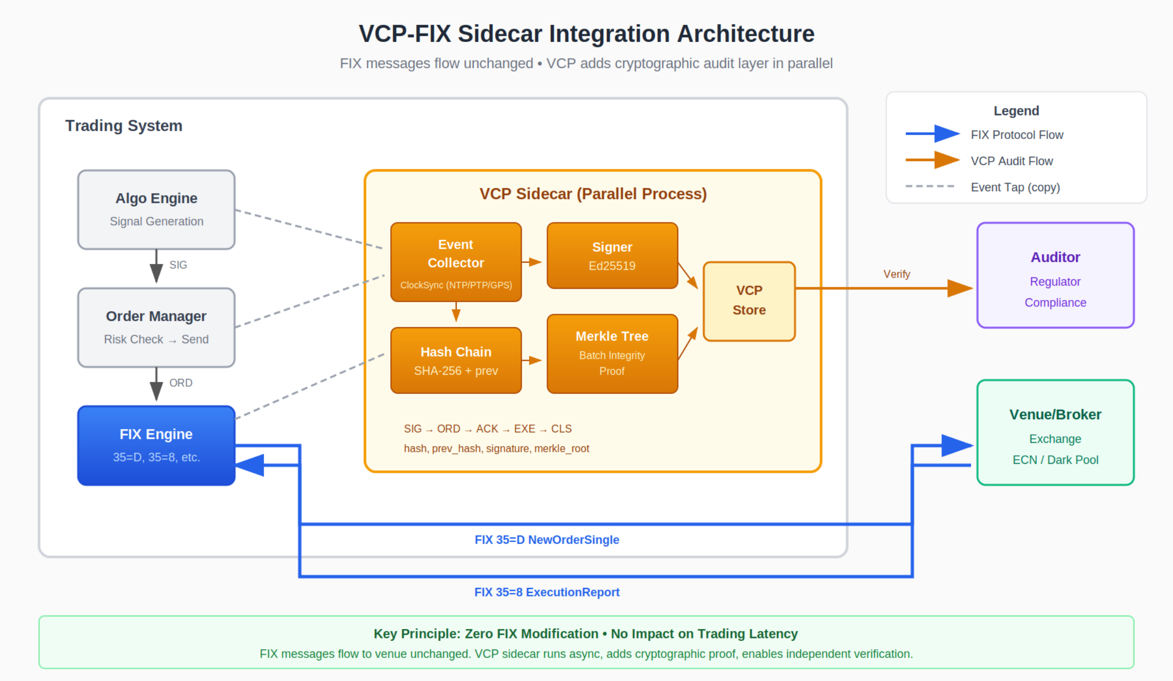
Proposed Tag	Name	Description
20010	AuditSignature	Ed25519/ECDSA digital signature
20011	AuditSignAlgo	Signature algorithm identifier
20012	AuditPublicKeyRef	Reference to signing key / certificate

Supports integration with RFC 3161 timestamping services or transparency logs.

3. Affected Message Types

MsgType	Message	Proposed Additions
D	NewOrderSingle	Clock sync, hash chain, AI decision
G	OrderCancelReplaceRequest	Clock sync, hash chain
8	ExecutionReport	Clock sync, hash chain, signature

4. Integration Architecture


VCP-FIX Sidecar Integration Architecture
FIX messages flow unchanged • VCP adds cryptographic audit layer in parallel
Trading System
Algo Engine
Signal Generation
SIG
Order Manager
Risk Check → Send
ORD
FIX Engine
35=D, 35=8, etc.
VCP Sidecar (Parallel Process)
Event Collector
ClockSync (NTP/PTP/GPS)
Signer
Ed25519
VCP Store
Hash Chain
SHA-256 + prev
Merkle Tree
Batch Integrity Proof
SIG → ORD → ACK → EXE → CLS
hash, prev_hash, signature, merkle_root
Legend
FIX Protocol Flow
VCP Audit Flow
Event Tap (copy)
Verify
Auditor
Regulator
Compliance
Venue/Broker
Exchange
ECN / Dark Pool
FIX 35=D NewOrderSingle
FIX 35=8 ExecutionReport
Key Principle: Zero FIX Modification • No Impact on Trading Latency
FIX messages flow to venue unchanged. VCP sidecar runs async, adds cryptographic proof, enables independent verification.

5. Recommended Next Steps

1. Working Group Discussion: Present to Algorithmic Trading WG for feedback
2. Industry Survey: Assess demand among FIX member firms
3. Regulatory Alignment: Coordinate with ESMA, SEC, FCA requirements
4. Draft Extension Pack: Develop formal EP proposal if interest confirmed

6. Reference Implementation

Open-source implementation: **VCP v1.0** (https://veritaschain.org) | IETF Draft: draft-kamimura-scitt-vcp | License: CC BY 4.0 / Apache 2.0

Contact: technical@veritaschain.org | standards@veritaschain.org | https://veritaschain.org

This document is provided for discussion purposes. It does not represent an official FIX Trading Community position.