FORENSICS ORACLE INITIATIVE
TECHNICAL BOARD · WORKING PAPER SERIES

TECHNICAL NOTE
FOI-TN-2026-001
Version: 1.0 · 17 August 2026
Classification: Public Reference

PUBLIC TECHNICAL REFERENCE · FOR INSTITUTIONAL REVIEW UNDER MICA, EIDAS 2.0 & EUROSYSTEM FRAMEWORK

Addressing the Physical Oracle Gap in MiCA-Compliant Real-World Asset Tokenization

A deterministic framework bridging judicial forensic practice, eIDAS 2.0 qualified signatures, and ERC-3643 smart contract circuit breakers for the physical verification of tokenized collateral.

AUTHOR
Forensics Oracle Initiative Technical Board

LEAD RESEARCHER
Aurelio Tamarit Blay · Judicial Expert Exp. No. 0161 · ORCID: 0009-0007-5824-3602

GOVERNING ENTITY
Aurema Group L.L.C. (Delaware, USA)

REGULATORY SUBMISSIONS
ESMA · EBA · EIOPA (confirmed) · ECB/SSM (ADITO portal)

1. Executive Summary

The Core Problem

Regulation (EU) 2023/1114 (MiCA) establishes comprehensive requirements for the tokenization of crypto-assets and Art-Referenced Tokens (ARTs), but **contains a structural blind spot**: it mandates reserve verification and custody safeguards without specifying how the **physical existence, structural integrity, and legal encumbrances** of Real-World Assets (RWAs) backing those tokens shall be deterministically verified.

We define this gap as the **"Physical Oracle Problem"** — the inability of distributed ledger technology (DLT) to attest to the physical state of off-chain assets without relying on centralized, unauditable data feeds.

The Proposed Solution

The **Prop Trust Verified Standard (PTVS v1.0)** introduces a deterministic three-pillar framework: (1) on-site forensic inspections by sworn judicial experts under eIDAS 2.0 qualified signatures, (2) off-chain SHA-256 canonical hashing for cryptographic lineage, and (3) on-chain Verifiable Claims injected via `PTVSClaimInjector` smart contracts with automated circuit breakers.

2. The Physical Oracle Problem

The European tokenization market has achieved regulatory clarity under MiCA, yet the **physical-digital bridge** remains architecturally under-specified. While price oracles (e.g., Chainlink, Pyth) provide market data feeds,

and identity oracles (e.g., ONCHAINID, T-REX) provide compliance verification, **no deterministic mechanism exists to verify the physical state of the underlying asset itself**.

2.1 Regulatory Gaps in Current Framework

REGULATION	REQUIREMENT	UNRESOLVED QUESTION
MiCA Art. 36 (Reserve Requirements)	Issuers of ARTs must maintain reserves "sufficient to cover claims" at all times.	How does the issuer *prove* the physical asset still exists and retains value?
MiCA Art. 45 (Custody Obligations)	Crypto-asset service providers must segregate and safeguard reserve assets.	What attestation mechanism validates physical integrity post-custody?
Solvency II Art. 84 (Prudent Person Principle)	Insurers must value investments with "appropriate methods" ensuring reliability.	How is physical degradation (e.g., structural pathology) reflected on-chain?
Guideline (EU) 2015/510 (Eurosystem Collateral)	Eligible collateral must meet "high credit standards" verified periodically.	What oracle attests to physical condition of real estate collateral?
eIDAS 2.0 Reg. 2024/1183 (Qualified Trust Services)	Qualified electronic signatures have equivalent legal effect to handwritten ones.	How is a qualified judicial attestation injected into DLT systems?

2.2 Failure Modes Without Physical Verification

Absent deterministic physical verification, the following failure modes emerge in RWA tokenization:
Structural degradation: A tokenized building develops aluminosis or reinforced concrete carbonation. The token continues trading at pre-degradation value.
Hidden encumbrances: A tokenized vessel is arrested in port under maritime lien. The token's smart contract shows no change in status.
Environmental damage: Tokenized agricultural land suffers soil contamination. The on-chain representation remains unchanged.
Insurance lapse: Physical asset loses insurance coverage. Token holders are unaware of increased risk exposure.

3. The PTVS v1.0 Deterministic Framework

PTVS v1.0 resolves the Physical Oracle Problem through a **three-pillar architecture** that combines judicial authority, cryptographic integrity, and smart contract automation.

3.1 End-to-End Verification Flow

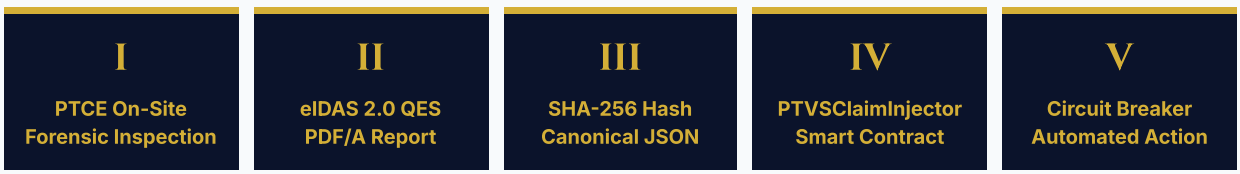

Figure 1 — Deterministic flow from physical inspection to on-chain Verifiable Claim.

3.2 Pillar I — eIDAS 2.0 Qualified Forensic Audits

On-site inspections are conducted exclusively by **Prop Trust Certified Experts (PTCEs)** — sworn judicial experts registered with their respective colegios profesionales in the EU. Each inspection produces:
A **PDF/A report** compliant with ISO 19005 (long-term archival)
A **Qualified Electronic Signature (QES)** under eIDAS 2.0 Regulation (EU) 2024/1183
A **RFC 3161 qualified timestamp** attesting to the precise moment of attestation
This ensures the inspection report carries **equivalent legal effect to a handwritten judicial report** in all EU Member States.

3.3 Pillar II — SHA-256 Cryptographic Lineage

The structured findings of the inspection are serialized into a **canonical JSON document** (deterministic key ordering, whitespace minimization) and hashed with SHA-256. The resulting hash is:
Deterministic: Any party can independently recompute it from the canonical JSON.
Tamper-evident: Any modification to the report changes the hash.
Off-chain anchored: Stored in CERN/Zenodo and HAL/CNRS for permanence.

3.4 Pillar III — Smart Contract Circuit Breakers

The `PTVSClaimInjector` smart contract (MIT-licensed, compatible with ERC-3643/T-REX) receives the Verifiable Claim and triggers **automated protective actions** based on the PTVS Score:

PTVS SCORE	STATUS	ON-CHAIN BEHAVIOR	REGULATORY IMPLICATION
70–100	VERIFIED	Full trading enabled; token accepted as eligible collateral.	Compliant with MiCA Art. 36 reserve requirements.
50–69	CONDITIONAL	Trading warnings; increased haircuts on collateral value.	Enhanced disclosure required under MiCA Art. 45.
0–49 (expired)	EXPIRED	Claim validity lapses; re-audit required within 90 days.	Asset no longer meets "periodic verification" under ECB Guideline.
Material degradation	REVOKED	**Circuit breaker activates:** trading paused, margin calls triggered, LTV auto-adjusted.	Immediate prudential action under Solvency II Art. 84.

3.5 Smart Contract Integration (ERC-3643/T-REX)

The `PTVSClaimInjector` is designed as a **complementary layer** to existing identity and compliance standards. Example integration:

```
// PTVSClaimInjector.sol — Simplified Interface
contract PTVSClaimInjector {
  struct VerifiableClaim {
    bytes32 assetId;
    uint8 ptvsScore;
    bytes32 forensicHash;
    uint256 inspectionTimestamp;
    address ptceAddress;
    ClaimStatus status;
  }

  function injectClaim(
    bytes32 assetId,
    uint8 score,
```

```
    bytes32 hash,
    bytes memory ptceSignature
  ) external onlyAuthorizedPTCE {
    // Verify PTCE identity via ONCHAINID
    // Inject claim into ERC-3643 token registry
    // Trigger circuit breaker if score < 70
  }
}
```

4. REGULATORY ALIGNMENT MATRIX

PTVS v1.0 is designed to operate **within** existing European regulatory frameworks, not to replace or compete with them. The following matrix maps PTVS capabilities to specific regulatory obligations:

REGULATORY FRAMEWORK	SPECIFIC OBLIGATION	PTVS V1.0 CONTRIBUTION
MiCA Regulation (EU 2023/1114)	Art. 36 — Reserve requirements for ART issuers	Deterministic attestation of physical existence and condition of reserve assets. PTVS Score provides quantitative metric for reserve adequacy.
MiCA Regulation (EU 2023/1114)	Art. 45 — Custody and segregation obligations	Periodic re-audits ensure custodial integrity over time. Expired claims trigger automatic disclosure requirements.
Solvency II Directive (2009/138/EC)	Art. 84 — Prudent person principle for investments	Forensic methodology aligns with "appropriate valuation methods" requirement. PTVS Score feeds into internal risk models.
IORP II Directive (2016/2341)	Art. 28 — Risk management for pension funds	Physical degradation alerts enable proactive risk mitigation in pension portfolios holding tokenized RWAs.
Eurosystem Collateral Framework (Guideline EU 2015/510)	Eligibility criteria for credit operations	PTVS Score ≥ 70 as potential eligibility criterion for tokenized real estate collateral in ECB liquidity operations.
eIDAS 2.0 (Regulation EU 2024/1183)	Qualified electronic signatures and trust services	All PTCE attestations use QES under eIDAS 2.0, ensuring cross-border legal admissibility in all EU Member States.
CRR III / Basel III (Regulation EU 2024/1156)	Capital requirements for credit risk	PTVS-verified collateral may qualify for preferential risk weights under standardized approach.
DLT Pilot Regime (Regulation EU 2022/858)	Sandbox for market infrastructure using DLT	PTVS v1.0 ready for integration into DLT-TSS (Trading and Settlement Systems) pilots.

5. SCIENTIFIC VALIDATION & PERMANENT REGISTRIES

PTVS v1.0 has been deposited in multiple permanent scientific registries to ensure **academic priority, reproducibility, and long-term preservation** independent of any commercial entity:

PERMANENT SCIENTIFIC REGISTRIES

CERN / ZENODO	DOI: 10.5281/zenodo.21719175 — Core Framework & Technical Specification
HAL OPEN SCIENCE	hal-05713062v1 — Computer Science Validation (CNRS, France)

OPEN SCIENCE FRAMEWORK	DOI: 10.17605/OSF.IO/7D2SJ — Reproducible Datasets & Smart Contracts
U.S. COPYRIGHT OFFICE	Cases 1-15210573311 (Theory) & 1-15234961091 (Solidity Contracts)
WIKIDATA ENTITY	Q140774713 — Named Entity for Knowledge Graphs
LEAD RESEARCHER ORCID	0009-0007-5824-3602 — Aurelio Tamarit Blay

5.1 European Regulatory Submissions

The complete PTVS v1.0 framework has been formally submitted to the four European Supervisory Authorities and the European Central Bank:

REGULATORY SUBMISSION REFERENCE NUMBERS

ESMA	FOI/ESMA/2026-001 — MiCA, DLT transparency, investor protection
EBA	FOI/EBA/2026-002 — CRR/CRD V, NPL mitigation, collateral inspections
EIOPA	FOI/EIOPA/2026-003 — Solvency II, IORP II — **Confirmed & Registered (11 Aug 2026)**
ECB / SSM	FOI/ECB-SSM/2026-004 — Eurosystem Collateral, Digital Euro — **Registered via ADITO portal**
INATBA	FOI/INATBA/2026-005 — RWA Working Group (application submitted)

6. Implementation Roadmap for Institutional Actors

6.1 For SSM-Supervised Banks

Phase 1 (Q4 2026): Join PTVS Technical Board as Founding Member to influence standard evolution.
Phase 2 (Q1 2027): Pilot PTVS integration on a controlled portfolio of tokenized collateral (target: €50-100M).
Phase 3 (Q3 2027): Production deployment for Eurosystem-eligible collateral with automated PTVS Score monitoring.

6.2 For MiCA-Licensed RWA Platforms

Phase 1 (Q4 2026): Obtain "Verified by PTVS" license and integrate Oracle API.
Phase 2 (Q1 2027): Certify first 10 assets under PTVS methodology; display widget to investors.
Phase 3 (Q2 2027): Scale to full portfolio; leverage PTVS Score as competitive differentiator in investor materials.

6.3 For Universities & Research Centers

Phase 1 (Q4 2026): Join Technical Board Academic seat; access PTVS datasets for research.
Phase 2 (2027): Co-author peer-reviewed publications on PTVS methodology and market impact.
Phase 3 (2027+): Offer PTVS certification training as continuing education for judicial experts.

> *"The blockchain guarantees that a transaction cannot be altered. But it cannot tell a supervisor whether the building backing that token has aluminosis, or whether the vessel complies with its class certificate. PTVS v1.0 bridges that gap with a deterministic, judicially-admissible, cryptographically-anchored framework."*
>
> — AURELIO TAMARIT BLAY, LEAD RESEARCHER, FORENSICS ORACLE INITIATIVE