IPAS Verification Standard: Infrastructure Physical Asset Standard for MiCA Article 36 Compliance and ERC-3643 Integration

Document Type: Technical & Architectural Proposal **Submitted to:** ERC-3643 Association | ESMA Digital Finance Contact Group **Author:** Petro Sidliarchuk, Structural Engineer CC3 (25 years experience, 157 buildings verified), InfraVeritas Protocol

---

Executive Summary

This document presents a comprehensive technical and architectural proposal for the implementation of the IPAS (Infrastructure Physical Asset Standard) verification standard — the first engineering framework system designed to provide continuous physical verification of tokenized Real-World Assets (RWA). The primary objective of this standard is to overcome a critical systemic vulnerability in the decentralized finance ecosystem, known as the "physical oracle problem," and to ensure full compliance with the strict regulatory requirements of the European Union, specifically Article 36 and Article 45 of the MiCA (Markets in Crypto-Assets) regulation.

While leading tokenization standards, such as the ERC-3643 protocol, have achieved unprecedented levels of sophistication in investor digital identity management (KYC/AML) and automation of on-chain asset transfer rules — securing infrastructure for assets worth over $32 billion — they remain blind to the physical condition of the underlying collateral. A smart contract cannot independently determine whether a building exists, whether its foundation is compromised, or whether the floor area matches what is stated in the emission prospectus (Whitepaper). The IPAS standard fills this gap by proposing a structured, risk-based physical inspection methodology that transforms analog engineering data into cryptographically secured, machine-readable attestations compatible with Chainlink Proof of Reserve (PoR) mechanisms and ERC-3643 compliance modules. This document is intended for protocol architects, smart contract developers, compliance officers, and regulatory bodies shaping the future of institutional digital assets.

1. Architecture of the Physical Oracle Problem in Web3

1.1. The Fundamental Gap Between On-Chain Data and Physical Reality

The integration of real-world assets into blockchain networks requires seamless synchronization between the state of an object in the physical world and its digital representation. This synchronization relies on oracles — systems that supply external data to smart contracts. However, while reliable cryptographically secured data feeds exist for financial instruments (e.g., exchange rates or stock prices), the so-called "last mile" problem remains unsolved for physical infrastructure and real estate. The physical oracle problem lies in the inability of current decentralized systems to guarantee that the physical object acting as collateral maintains its integrity, meets stated specifications, and actually exists at the specified coordinates at the time of the transaction.

Historical precedents in the decentralized finance market clearly illustrate the catastrophic consequences of ignoring this issue. Projects like MANTRA/OM have demonstrated the vulnerability of systems where billions of dollars in tokenized value relied on unverified or static claims regarding physical collateral. A similar situation occurred with the Tangible protocol and their USDR token, which was backed by UK real estate: tokens continued to be actively traded on secondary markets and used as collateral in lending protocols, while the actual physical real estate had already degraded or lost liquidity.[1] In both cases, the smart contracts functioned perfectly from a code perspective, but the underlying asset they relied upon was compromised. This proves that a digital asset wrapper cannot be more reliable than the physical object at its core.

1.2. Inefficiency of Existing Audit Paradigms

Traditional approaches to verification and auditing currently applied in the Web3 industry are fragmented and conceptually unsuited to solve the physical oracle problem. An analysis of the current landscape reveals critical gaps in each existing methodology.

Verification Methodology	**Audit Focus and Scope**	**Systemic Gaps and Flaws**
Smart Contract Audit (e.g., Hacken, Certik)	Solidity code correctness, reentrancy resistance, logical access control	Complete lack of verification of the collateral's physical existence, structural condition, and real value
Traditional Real Estate Appraisal	Determination of market value at a single static point in time (usually before emission)	Ignoring hidden structural defects, lack of monitoring of construction progress and depreciation

Centralized Audit Reports (PDF)	Issuer's financial health (balance sheet), confirmation of legal ownership	Lack of on-chain integration, impossibility of cryptographic proof, lack of continuous monitoring
Self-Reported Net Asset Value (NAV)	Accounting and financial reporting provided by the issuer itself	Lack of independent expertise, high risk of data manipulation, ignoring physical condition

The inefficiency of these approaches is particularly acute in sectors with high value dynamics, such as construction lending (bridge loans or fix-and-flip models). In these scenarios, the underlying asset is a real estate object undergoing active renovation or construction. Its actual market value at any intermediate point may be only 30-50% of the stated After Repair Value (ARV) hardcoded into the token's metadata. Without a continuous flow of verified engineering data, a smart contract cannot recalibrate the collateral value, leading to systemic undercollateralization of the lending pool and creating conditions for protocol insolvency in the event of mass withdrawals.

2. Regulatory Imperative: MiCA, RTS, and EBA/ESMA Prudential Requirements

2.1. Requirements of Article 36 and Article 45 of the MiCA Regulation

The European Markets in Crypto-Assets (MiCA) regulation establishes a new era of institutional responsibility for digital asset issuers. Article 36 (Title III, Chapter 3) strictly regulates the obligations regarding the creation and management of an asset reserve for issuers of Asset-Referenced Tokens (ART). Under these rules, issuers must not only form a reserve but also ensure its prudent management, continuous assessment, and protection of token holders' interests. For protocols issuing ARTs based on physical infrastructure or real estate, this translates into a direct legal obligation to prove that the physical asset actually exists at the stated coordinates, its current parameters fully match the specifications published in the crypto-asset Whitepaper, and its structural condition does not threaten the reserve's value.

Additionally, Article 45 of the MiCA regulation imposes ongoing obligations for continuous monitoring of reserve assets and transparent updates to investor disclosures. This means the "fire-and-forget" paradigm (verifying once at issuance) is no longer legally acceptable. The regulator requires dynamic oversight capable of detecting changes in the asset's risk profile in real-time.

2.2. EBA Prudential Stance on Liquidity Reserves (2025-2026)

The European Banking Authority (EBA) plays a key role in developing regulatory technical standards (RTS) that detail MiCA requirements. In its Opinions EBA/Op/2025/13 and EBA/Op/2025/14, published in late 2025 and early 2026, the EBA demonstrated an uncompromising stance on the quality of reserve assets. The EBA sharply criticized the European Commission's attempts to relax requirements for Highly Liquid Financial Instruments (HLFI). Specifically, the EBA warned that classifying commodities, illiquid assets, or crypto-assets as HLFIs, and relaxing concentration limits, is a direct violation of MiCA's prudential framework (specifically Articles 36(1)(b) and 38(1)) and opens the door to regulatory arbitrage and systemic liquidity risks.

For the RWA industry, this has profound implications. Because tokenized real estate and infrastructure are inherently not highly liquid instruments with minimal market risk, issuers of ARTs backed by such assets fall under the most stringent requirements for liquidity management and reserve stress testing. If the physical asset in the reserve suffers hidden degradation (e.g., critical damage to load-bearing structures), its actual liquidation value drops. If the issuer fails to detect this in time due to the lack of a physical verification standard, they automatically violate EBA liquidity ratios (e.g., the requirement to maintain own funds at 3% of the average reserve amount for significant ARTs), which can lead to penalties and suspension of operations. The IPAS standard is specifically designed to provide issuers with the continuous flow of reliable engineering data required to correctly perform calculations under the EBA methodology.

2.3. ESMA Technical Reporting Formats (iXBRL)

The European Securities and Markets Authority (ESMA) imposes strict requirements on the data submission format. According to ESMA's implementing technical standards developed in 2024-2025, all crypto-asset Whitepapers must be published in the machine-readable Inline XBRL (iXBRL) format. This format combines visual representation in an XHTML document with embedded XBRL tags, allowing regulators to automatically extract and analyze financial and operational metrics. The IPAS standard is designed with this requirement in mind: physical inspection results (geometric parameters, condition assessments, consequence class data) are structured so that they can be directly integrated into relevant XBRL taxonomies, minimizing human error in regulatory reporting preparation and ensuring full compliance with ESMA transparency requirements.

3. IPAS Engineering Methodology: Five Critical Verification Nodes

The IPAS standard moves away from superficial visual inspections and introduces a deep structural methodology based on European design standards (Eurocodes) and Consequence Classes. IPAS version 1.0 is designed for CC1 (warehouses, agricultural buildings) and CC2 (standard residential and commercial real estate) class objects. CC3 class assets (strategic infrastructure, bridges, high-rise complexes) are subject to even stricter protocols requiring panels of senior experts, which will be regulated in version 2.0. The foundation of the methodology is a detailed analysis of five structural nodes. A failure in any of these nodes inevitably leads to a total or significant loss of asset value, directly threatening the solvency of the backed token.

Node 1: Foundation and Geotechnical Stability

The foundation is the absolute basis of any physical asset. A compromised foundation means total loss of the object. A building with impaired geotechnical stability is uninsurable, unsellable on the open market, and cannot serve as collateral for refinancing. In the context of RWA, this means the token's intrinsic value instantly drops to zero, creating a systemic threat if these tokens continue to trade or be used as collateral in DeFi protocols. Node 1 inspection includes precise measurement of differential settlement, analysis of crack width, detection of moisture intrusion zones, and assessment of reinforcement condition.

Foundation Degradation Indicator	**Threshold for Trigger Activation**	**Direct Regulatory and On-Chain Impact (MiCA)**
Differential (Uneven) Settlement	Visible structural tilt or measured difference >15 mm	Immediate requirement for reserve revaluation, potential trading halt
Structural Crack Width	Hairline <0.3 mm (monitor); Active >0.6 mm (critical)	Mandatory senior engineer review, smart contract status update
Moisture Intrusion and Efflorescence	Active water seepage or persistent staining patterns on walls	Initiation of accelerated quarterly re-inspection protocol
Exposed Reinforcement Framework	Any visually confirmed corrosion of working rebar	Immediate engineering assessment of residual load-bearing capacity

Node 2: Load-Bearing Structure (Structural Frame)

The structural frame determines the safety, useful life, and maximum load capacity of a building. For commercial real estate tokenized for rental income, any reduction in permitted floor payload directly limits the pool of potential tenants (e.g., inability to host heavy equipment or archives), which automatically reduces the asset's yield. Verifying this node requires deep instrumental analysis. For steel structures, IPAS engineers check for cross-sectional area loss due to corrosion (acceptable limit <10%), signs of buckling, weld integrity, and protective coating delamination. For concrete frames, crack mapping, checking concrete cover thickness, and chemical tests (e.g., phenolphthalein method to determine concrete carbonation depth in CC2+ assets) are mandatory. Additionally, spot checks of bolt torque in critical primary connections are conducted.

Node 3: Roof and Envelope Systems

Contrary to popular belief, roof system failure is the most common cause of sudden and rapid value loss in commercial real estate. Localized roof sagging leads to ponding water zones. Each such pool creates an unplanned static load of 0.8-1.0 kN/m, which can lead to progressive failure of load-bearing beams. Furthermore, a polymer membrane that visually appears intact may have lost up to 80% of its designed service life under UV exposure, requiring multi-million dollar capital investments not accounted for in the token's financial model.

Envelope Degradation Indicator	**Instrumental Detection Method**	**Economic and Structural Consequences for RWA**
Ponding Water Zones on Roof	Drone thermal imaging or post-rainfall inspection	Structural overload risk, potential loss of 15-40% of market value
Roof Membrane Delamination	Core sampling or infrared thermal scanning	Full roof replacement cost ranges from 3% to 8% of total asset value
Facade Anchor System Failure	Visual inspection and acoustic tapping of representative panels	Risk of emergency public closure, rental income drops to zero

Penetration Seal Failure	Total visual inspection of all MEP penetrations	Uncontrolled water intrusion, accelerating Node 1 and Node 2 degradation scenarios

Node 4: MEP Systems (Mechanical, Electrical, Plumbing)

For tokenized assets, the capacity and condition of engineering systems must strictly and uncompromisingly align with the business model stated in the Whitepaper. The problem is that transforming a standard warehouse into a data center or pharmaceutical cold storage complex radically alters MEP requirements. If the facility lacks verified three-phase power of adequate capacity, backup generators, or if the HVAC systems cannot provide the required air changes per hour and specific cooling capacity (kW/m^2), the asset's financial model becomes non-viable. In such a case, the stated yield is a fiction, and the token value is artificially inflated, directly violating MiCA reserve management principles. IPAS requires verification of HVAC parameters, transformer load capacity checks, and hydraulic testing of commercial-grade plumbing systems.

Node 5: Geometric Compliance and Spatial Parameters

Overstating usable floor area is the most common method of value manipulation in the real estate tokenization sector. The mathematics of this risk are linear: a 10% discrepancy in stated floor area automatically generates a 10% non-existent ("air") asset value. When this error scales across an investment pool of 50 or more properties, it leads to massive investor deception and artificial market cap inflation. The IPAS protocol eliminates this risk by introducing strict tolerances. Gross floor area measurements using laser distance meters (Leica Disto class) must match the technical passport within a ±2% tolerance. Net usable area is verified with a ±3% tolerance against smart contract parameters, while ceiling heights and column grids are verified down to the centimeter.

4. Monitoring Dynamics: Risk-Based Inspection Frequency

Static audits do not align with the nature of physical objects. In accordance with MiCA Article 45 requirements for continuous monitoring and issuer obligations to promptly update information , IPAS introduces a dynamic, differentiated inspection schedule. Frequency is determined by the specific nature of the object, the intensity of its operational loads, and its consequence class.

Asset Classification by Type	Example Objects	IPAS Mandated Frequency	Engineering Rationale for Schedule
High-Load Industrial Facilities	Logistics hubs, manufacturing plants, factories	Every 3 years	Systematic vibration exposure from heavy equipment, high transport floor loading, accelerated wear
General Purpose Commercial Real Estate	Shopping centers, CC2/CC3 office buildings	Every 5 years	Compliance with municipal public building safety standards, stable wear cycles
Residential Real Estate (Mortgage Pools)	Multi-family residential complexes	Every 5-10 years	Significantly lower operational and wear intensity compared to the industrial sector
Critical and Strategic Infrastructure	Bridges, ports, hyperscale data centers	Annually (baseline visual) + Every 5 years (deep instrumental)	Highest potential for catastrophic consequences to reserve stability; any failure means immediate total loss
Construction Projects and Renovation (Fix-and-Flip)	Bridge loan assets, active renovation projects	At each funding stage (tranche) + before commissioning	Asset value is dynamically formed as work progresses. Strict synchronization of on-chain valuation with physical progress

In addition to scheduled inspections, the standard defines a list of extraordinary triggers requiring immediate ad-hoc verification. These include: seismic activity (magnitude >4.5 within

50 km of the object), flooding reaching the building perimeter, fires of any scale, unauthorized capital works, changes in the object's intended use, and the registration of official insurance claims. Information about these events automatically triggers the suspension of the previous attestation until a new audit is completed.

5. Cryptographic Evidence Framework

For engineering data to function as a reliable oracle in a decentralized system, it must be tamper-proof, cryptographically verifiable, and easily integrated into on-chain ledgers. IPAS introduces a four-layer evidence collection and processing architecture that produces attestations compatible with key Web3 infrastructures.

Layer 1: Spatial Digital Twin (LiDAR)

The primary evidence of physical existence and geometric integrity is a millimeter-accurate 3D model of the object, created using LiDAR laser scanning. For CC1 and CC2 class assets, the protocol permits consumer-grade LiDAR devices (e.g., iPhone Pro with verified Polycam or Matterport APIs), while CC3 requires specialized surveying equipment. The generated 3D model is cryptographically hashed, the resulting hash is stored in the IPFS distributed file system, and the corresponding link is recorded on the smart contract with a timestamp. This allows auditors and regulators to remotely verify spatial dimensions and, critically, detect structural micro-deformations over time by overlaying the current scan onto the baseline model.

Layer 2: BIM Integration and Immutable Audit Trail

Any changes in the asset's physical state discovered during inspections are entered into the Building Information Model (BIM). Each entry is accompanied by a timestamp and the digital signature of the responsible engineer. This mechanism creates a continuous, immutable audit trail that perfectly satisfies MiCA Article 45 requirements for continuous oversight. Regulatory bodies gain the ability to trace the complete ontology of the asset — from its initial tokenization through all operational cycles to its current state.

Layer 3: Licensed Engineer Attestation (PE Stamp)

This is the core of trust in the IPAS protocol. Unlike anonymous or semi-anonymous smart contract auditors, physical verification under the IPAS standard must be signed by a licensed structural engineer with the appropriate clearance level from state regulatory bodies. The engineer's seal (PE Stamp) shifts the responsibility for data accuracy from the realm of financial slashing into the realm of strict legal liability. If an engineer attests to false data regarding a building's foundation integrity, they risk not only their reputation but face lifetime revocation of their professional license and criminal prosecution under EU or US law. Acceptable qualifications include: Professional Engineer (PE) in the US, Chartered Engineer (CEng) in the UK, Anerkendt statiker in Scandinavia, or Bauingenieur in Germany. This legal deterrent is vastly more powerful than any financial slashing mechanism in traditional blockchain networks.

Layer 4: Secured Visual Evidence and GPS Telemetry

All visual materials (photos and videos) collected during the inspection are enriched with EXIF metadata containing immutable GPS coordinates and timestamps. The system automatically cross-references these coordinates against the address hardcoded in the smart contract (with a strict ±100-meter tolerance). Timestamps are verified against the inspection request initiation date (±48 hours tolerance). To counter "replay" attacks (reusing old photographs), perceptual hashing (pHash) algorithms are applied. Furthermore, LiDAR scanning sessions are device-signed metadata, making post-processing or tampering with scans mathematically impossible.

6. Protocol Integration: Smart Contracts and ERC-3643 Compatibility

To ensure liquidity, tokenized assets must operate within a standardized environment. Currently, the de facto standard for issuing regulated securities and permissioned tokens on the Ethereum network is ERC-3643 (formerly T-REX). This protocol supports over $32 billion in tokenized value, spans 180+ jurisdictions, and enforces complex compliance logic via decentralized identity (ONCHAINID). The IPAS standard is natively designed as a "physical compliance extension" for the ERC-3643 ecosystem.

6.1. Interaction Architecture with ERC-3643 Modules

The ERC-3643 protocol is based on a strict separation of token logic (ERC-20), identity management (IIdentityRegistry), and compliance rules (IModularCompliance).

IPAS integration works as follows:

1. **Asset Identification:** The ONCHAINID system is traditionally used to store investor KYC status. In the IPAS architecture, the physical asset itself receives its own ONCHAINID smart contract. This decentralized identifier accumulates all cryptographic claims regarding the object's condition.
2. **Claim Issuance:** Licensed IPAS engineers are registered in the ITrustedIssuersRegistry contract as trusted issuers of specialized claims (e.g., "Structural Integrity Attestation"). Upon completion of an inspection, the engineer publishes the signed claim to the asset's ONCHAINID using the IClaimTopicsRegistry.
3. **Automated Transfer Blocking:** The IModularCompliance contract intercepts every token transfer attempt between users. It queries the asset's ONCHAINID and checks the IPAS physical attestation status. If the conditionScore parameter equals 5 (Critical) or if the attestation has expired (nextVerificationDue is overdue), the isVerified() function returns false, and the smart contract automatically reverts the transaction. This is a revolutionary mechanism that instantly blocks the trading of toxic or degraded assets on decentralized

exchanges, protecting the secondary market.

Base ERC-3643 Functionality	**Extension via IPAS Standard**
Investor Identity Management (KYC/AML) via ONCHAINID	Creation of a digital identity for the physical asset itself, recording geolocation and consequence class
Transaction Restrictions Based on Sanction Lists or Holding Limits	Strict transaction blocking upon detection of critical physical degradation (conditionScore = 5)
Utilizing Trusted KYC Providers as Claim Issuers	Integration of a decentralized network of licensed structural engineers
Compliance Module Updates Due to Financial Law Changes	Dynamic token status updates based on routine or extraordinary inspection results

6.2. Chainlink Proof of Reserve (PoR) Compatibility

For decentralized lending protocols (DeFi), such as Aave, Morpho, or MakerDAO, it is critical to receive standardized collateral value data. The IPAS attestation is formatted as a Data Feed compatible with the Chainlink PoR mechanism.

The Solidity struct looks like this:

- assetId (bytes32): Unique identifier linked to the asset's ONCHAINID.
- verificationTimestamp (uint256): Inspection execution time.
- conditionScore (uint8): Rating from 1 (Excellent) to 5 (Critical).
- geometricCompliance (bool): Confirmation that actual floor area matches stated area within ±3%.
- evidenceHash (bytes32): IPFS hash of the evidence package (LiDAR, BIM, PE-stamped PDF report).

This standardized data stream allows lending protocols to automatically liquidate loans or demand additional collateral if the physical condition of the collateral deteriorates.

7. Decentralized Consensus: Proof of Expertise (PoE) and CVR

Relying on a single centralized audit firm contradicts the foundational principles of Web3 and creates a single point of failure. The IPAS architecture solves this problem by building a decentralized Witness Network of engineers operating on a "Proof of Expertise" (PoE) consensus mechanism.

7.1. PoE vs. Classical Proof of Stake (PoS)

In PoS networks, security is guaranteed by financial capital (cryptocurrency staking), which is slashed in the event of malicious behavior. However, for real-world verification, financial penalties are insufficient. A malicious engineer could receive a bribe significantly exceeding their financial stake. In the PoE model, the underlying asset is the expert's reputation and legitimate state license, represented as a non-transferable Soulbound Token (SBT).

Consensus Characteristic	**Proof of Expertise (PoE)**	**Classical Proof of Stake (PoS)**
Base Asset for Validation	State engineering license + impeccable professional reputation (SBT)	Liquid crypto-assets (e.g., ETH, USDT)
Slashing Vector	Lifetime network exclusion + initiation of legal investigation risking professional license	Confiscation of a portion of locked financial funds
Deterrent Effectiveness	Absolute: risk of career destruction and criminal liability	Relative: losses are strictly limited to stake size
Sybil Attack Resistance	Maximum: one physical person with a unique license equals one identity	Dependent on token distribution; large capital can spin up numerous nodes

7.2. Continuous Verifiable Reality (CVR) and Selection Algorithms

For each inspection, the network selects a panel of certified engineers with the required clearance class (e.g., CC2 or CC3) using a Verifiable Random Function (VRF), making collusion between the issuer and inspectors impossible. The voting process for the conditionScore is anonymous. In phase 3 of the protocol, Zero-Knowledge Proofs (ZKP) will be implemented to fully obfuscate the decision-making process until the final consensus is committed.

To calculate data reliability and manage voting weights, the Continuous Verifiable Reality (CVR) framework is employed. The CVR model utilizes a complex system of weighting parameters :

- **Accuracy ($\alpha = 0.4$):** Highest weight, ensuring the integrity of engineering calculations.
- **Uptime ($\beta = 0.3$):** Incentivizes engineers to provide continuous data streams in a timely manner.
- **Stake ($\gamma = 0.2$):** Moderate financial component preventing pure plutocracy within the network.
- **Dispute Penalty ($\delta = 0.1$):** Mechanism for immediate node rating reduction if found participating in falsified or contested verification rounds.

This approach fully aligns with upcoming industry standards, notably the Royal Institution of Chartered Surveyors (RICS) Standard on AI in Surveying Practice, effective March 2026. Under this standard, AI and automated monitoring systems in IPAS act solely as pre-filters and anomaly analyzers, while final consensus and professional liability always remain with the panel of live certified engineers.

8. Strategic Integration and Piloting Proposals

This document forms the foundation for the practical implementation of the IPAS standard into key infrastructure ecosystems and the European regulatory framework. We propose a three-tier adoption strategy.

8.1. Strategic Proposal to the ERC-3643 Association

We appeal to the ERC-3643 Association to adopt the IPAS standard as an official and standardized Physical Compliance Extension for the T-REX protocol. Given that the GT4 working group of the ISO TC 307 committee is currently actively promoting ERC-3643 as a global international ISO standard for securities tokenization , the lack of a standardized physical verification mechanism remains its only structural flaw. Furthermore, the recent addition of the Depository Trust & Clearing Corporation (DTCC) to the Association aimed at integrating ERC-3643 into the ComposerX platform requires an unprecedented level of risk management. Implementing IPAS will allow DTCC and other institutional players to not only manage ownership rights on-chain but also obtain cryptographic guarantees regarding the condition of underlying assets. We propose the joint development of reference smart contract interfaces that will allow existing issuers (on platforms like Tokeny, etc.) to plug IPAS data feeds into their modules on a plug-and-play basis.

8.2. Submission to the ESMA Digital Finance Contact Group

The IPAS standard is officially submitted as a technical reference model to the Digital Finance Contact Group at ESMA. The goal of this submission is not to seek licensing for the IPAS protocol itself (which is a decentralized infrastructure), but to demonstrate to the regulator that a viable, mathematically and engineeringly sound methodology exists in the market, capable of satisfying the requirements of MiCA Articles 36 and 45 regarding reserve asset assessment. ESMA's recognition of the IPAS methodology will allow hundreds of European RWA issuers to use this standard to prove "prudent management" of assets during audits and avoid sanctions for violating liquidity limits warned about by the EBA. The use of licensed engineers (PE Stamp) creates a chain of professional accountability that fully satisfies the institutional requirements of European financial regulators.

8.3. Launch of a Pilot Validation Program

To empirically confirm the architecture's viability, the IPAS protocol initiates a pilot project based on real-world assets already existing within the infrastructure of leading RWA protocols (such as Centrifuge, Blocksquare, or Tokeny infrastructure solutions).

The pilot project design entails:

- Selecting 3 to 5 physical properties (CC1/CC2) that are already tokenized or pending emission in a partner's pool.
- Conducting a full inspection cycle (Nodes 1-5) utilizing LiDAR modeling and involving certified engineers.
- Issuing "Physical Asset Attestations" in a Verifiable Credentials format compatible with the ERC-3643 standard.
- Configuring the transmission of this data via oracle infrastructure (Data Feed) in Chainlink PoR format.
- The pilot deployment will last 4-6 weeks. The IPAS protocol absorbs all operational and engineering costs in exchange for the partner's agreement to publish a detailed open case study validating the methodology. This report will serve as empirical proof that the physical oracle problem can be successfully resolved at an industrial scale.

Signed by: Petro Sidliarchuk Structural Engineer CC3 InfraVeritas Protocol