FeedOracle Whitepaper

Evidence-Grade Data Infrastructure for Regulated Workflows

Version 3.2 · February 24, 2026

Download as PDF

API Docs →

DOCUMENT CONTROL

Version	3.0.0
Date	14 February 2026
Status	Published

Changelog v3.2 (Feb 24, 2026): Architecture updated to CORE + 4 Modules + MCP. Added Verified Reports, Payment Infrastructure, A2A Monetization, Report Verification to Delivered. New "In Progress" roadmap section. Regulatory source citations added to Legal. Proof wording standardized (XRPL live, Polygon deployed). SOC 2 status updated to Audit-ready. Version synchronized across all formats.

Table of Contents

1. Product Overview

FeedOracle is evidence-grade data infrastructure for regulated workflows. The platform delivers multi-source risk intelligence for tokenized assets — with every API response cryptographically signed and anchored on-chain for auditability.

The platform is built on a **one core engine, four compliance modules + AI agent layer** architecture:

COMPONENT	ROLE	PURPOSE	KEY OUTPUT
RWA Risk Oracle	⚡ **CORE**	Multi-dimensional risk scoring for 61+ tokenized asset protocols across 9 vectors	Composite risk scores, anomaly detection, yield analysis

MiCA Regulatory Evidence	📋 Module 1	Structured compliance metadata for EU MiCA/DORA workflows	Le… ju… identifier registry
Carbon & ESG Context	🌱 Module 2	Per-chain carbon footprint with ISO 14040 methodology	CO_2 metrics, green scores, CSRD-ready ESG output
DORA Compliance	🛡️ Module 3	Digital Operational Resilience Act evidence infrastructure	ICT incident reporting, vendor risk assessment, business continuity evidence
CSRD/ESRS Reporting	📊 Module 4	Corporate Sustainability Reporting with 5 dedicated APIs	EU Taxonomy, materiality, emissions, social metrics, governance
MCP Server	🤖 Agent Layer	Model Context Protocol with 18 tools for AI agents	Pre-trade compliance, MiCA status, custody risk, evidence generation

All components share a common evidence layer: ECDSA-signed responses, SHA-256 hashing, Evidence Pack Manifests (EPM), and on-chain anchoring (XRPL live per-transaction, Polygon contract deployed). The platform runs **48+ production services** across 4 compliance modules.

Core Principles

- **Data infrastructure, not advisory.** FeedOracle delivers structured data and verifiable evidence artifacts. Compliance decisions remain with the institution and its qualified advisors.
- **Source transparency.** Every data point traces back to documented institutional sources with published methodology.
- **Cryptographic verifiability.** Every API response is ECDSA-signed with publicly discoverable keys (JWKS).
- **EU-based operations.** Primary infrastructure hosted in Germany. Subprocessor register available.

FeedOracle is an independent infrastructure provider with no formal affiliation with any blockchain network, issuer, or regulator referenced in this document.

2. Executive Summary

Regulated institutions entering tokenized assets face a data gap. MiCA introduces disclosure requirements for CASPs (transitional period ends June 2026; stablecoin rules already in force). DORA raises expectations around operational traceability. CSRD/ESRS requires ESG reporting. Yet no infrastructure delivers risk intelligence for RWA protocols with the evidence trail that institutional workflows demand.

FeedOracle closes this gap with three capabilities:

1. **Multi-source risk scoring** — 61 RWA protocols and 105+ stablecoins scored across 9 independent risk dimensions from 5 data sources, enriched with FRED macro economic benchmarks.
2. **Regulatory evidence** — MiCA compliance for 105+ stablecoins (Significant Issuer detection, reserve drift monitoring, interest scanning), DORA operational resilience (incident reporting, vendor risk, business continuity), CSRD/ESRS reporting (5 APIs), ISO 20022 validation — structured for audit-ready workflows.
3. **Delivery proof** — Every data point wrapped in ECDSA-signed Evidence Packs with SHA-256 hashing, JWKS-verifiable signatures, and on-chain anchoring (XRPL live, Polygon deployed).
4. **AI agent access** — MCP Server with 18 compliance tools for Claude, Cursor, and autonomous agents. Live on Olas Mech marketplace (Gnosis) with 133+ verified deliveries.

The result: institutions can integrate verifiable risk data into their existing compliance workflows without building the data infrastructure themselves.

3. The Problem

The Disclosure Gap

Financial institutions evaluating tokenized assets need risk data that meets institutional standards. Current blockchain data providers focus on DeFi price feeds

and analytics — not on the structured, evidence-grade data t
requirements. The VASP transitional deadline (June 2026) creates
CASPs, exchanges, and DeFi protocols.

Missing Audit Trail

When auditors ask "Can you prove what data you used for this decision?", traditional API calls leave no verifiable trail. Screenshots and PDF attestation reports are not machine-readable, not verifiable, and not auditable. Institutions need cryptographic evidence of data delivery.

Procurement Friction

Enterprise procurement requires: EU data residency documentation, incident management procedures, subprocessor registers, SLO evidence, and exit strategies. Few blockchain data providers deliver this level of operational documentation.

Fragmented Intelligence

Assessing a single RWA protocol today requires pulling data from 5+ independent sources (on-chain metrics, market data, macro indicators, regulatory databases, ESG scores), normalizing it, and creating a defensible risk view. This is expensive and error-prone when done manually.

4. The Solution

PROBLEM	FEEDORACLE SOLUTION
No unified RWA risk view	61 RWA protocols & 105+ stablecoins scored across 9 risk dimensions from 5 data sources, enriched with FRED macro benchmarks
Missing audit trail	ECDSA-signed Evidence Packs with SHA-256 hashing, JWKS verification, and on-chain anchoring (XRPL live, Polygon deployed)
Fragmented regulatory data	MiCA compliance (105+ stablecoins, Art. 44 Significant Issuer, Art. 25 reserve monitoring), DORA (3 APIs), CSRD (5 APIs), ISO 20022 — unified evidence infrastructure

Enterprise procurement barriers	EU-hosted infrastructure, documented controls, subprocessor register, SLO evidence
No machine-readable compliance	REST APIs with consistent JSON schemas, OpenAPI 3.0 specification, configurable policy outputs

5. CORE — RWA Risk Oracle

The RWA Risk Oracle is FeedOracle's core product. It provides real-time multi-dimensional risk scoring for tokenized asset protocols, designed for institutional portfolio assessment, due diligence, and ongoing monitoring.

Coverage

The oracle currently scores **61 RWA protocols** and monitors **105+ stablecoins** across **12 jurisdictions** from **5 independent data sources**. Coverage spans regulated stablecoins, tokenized treasuries, private credit, real estate, commodities, equities, insurance, and XRPL native assets.

> **Methodology note:** TVL figures are sourced from DeFiLlama and reflect aggregate protocol TVL at time of data refresh (daily). Full methodology available at docs/methodology.

9 Risk Dimensions

Every protocol is scored across 9 independent dimensions, each sourced from verified institutional data providers:

📊 TVL Weight
Protocol scale & concentration
Source: DeFiLlama

📈 Yield Spread
Deviation vs. T-Bill benchmark
Source: FRED

🔀 Diversification
Chain & asset mix (HHI analysis)
Source: On-chain

Protocol age & track record

Source: On-chain

Regulatory

Jurisdiction risk flags

Source: Regulatory registers

Known institutional participants

Source: Public disclosures

💧 DEX Liquidity

Secondary market depth

Source: GeckoTerminal

⛓ On-Chain Activity

Transaction patterns & health

Source: Etherscan, Ankr

🌱 ESG / Carbon

Sustainability indicators

Source: CCRI, EMBER

Scoring Methodology

Each dimension produces a normalized score (0–100). The composite risk score is a weighted aggregate with configurable weights per institutional use case. Default weights are published in the API documentation. Scores are deterministic: the same input data always produces the same output score.

Anomaly Detection

Z-score outlier analysis flags unusual protocol behavior across all dimensions. Configurable alert thresholds enable automated monitoring and early warning signals for portfolio risk management.

Macro Economic Enrichment

The CORE engine is enriched with macro economic data from FRED (Federal Reserve Economic Data), ECB, and World Bank. This enables yield-spread analysis against T-Bill benchmarks, credit spread monitoring, recession probability indicators, and economic health indices — providing institutional context for RWA risk assessment.

Key Endpoints

ENDPOINT	METHOD	DESCRIPTION
/v1/rwa/risk	GET	All scored protocols with composite scores

/v1/rwa/risk/{slug}/pdf	GET	PDF evidence report
/v1/rwa/market	GET	Aggregate market view
/v1/macro/indicators	GET	Macro economic enrichment

6. MODULE 1 — MiCA Regulatory Evidence

Module 1 provides the most comprehensive MiCA compliance infrastructure available. It covers **105+ stablecoins** with real-time peg monitoring, reserve drift detection, significant issuer classification (Art. 44), interest prohibition scanning (Art. 23/52), document compliance verification (Art. 29/30/55), and ESMA register mirroring — plus legal state analysis, jurisdiction mapping, and CCI scoring. All outputs are Evidence Pack-wrapped for audit trails.

> **Regulatory context:** MiCA CASP transitional period ends June 30, 2026 (stablecoin rules already in force since June 2024). Exchanges, CASPs, and DeFi protocols handling EU-regulated crypto-assets need machine-readable compliance data. Module 1 provides the evidence artifacts.

6.1 Legal State Analysis

Contract Powers & Ownership

`Source: On-chain governance analysis, public disclosures`

Analysis of smart contract governance structures, ownership patterns, upgrade mechanisms, and dispute resolution paths. Returns structured metadata for regulatory due diligence.

Endpoint: `GET /v1/rwa/legal-state/{slug}`

6.2 Jurisdiction Mapping

12 Jurisdictions + Sanctions Screening

`Coverage: 12 jurisdictions · OFAC, EU, UN sanctions lists`

Maps RWA protocols to their operating jurisdictions and screens against OFAC, EU, and UN sanctions lists. Returns jurisdiction risk flags, regulatory regime classification, and cross-border compliance indicators.

Endpoint: `GET /v1/rwa/compliance/{slug}`

6.3 Identifier Registry

LEI, ISIN/CUSIP, Custody Details

`Source: Regulatory registers, public filings`

Registry of institutional identifiers for RWA protocols: Legal Entity Identifiers (LEI), ISIN/CUSIP mappings, custody provider details, and issuer metadata. Machine-readable for compliance system integration.

Endpoint: `GET /v1/rwa/registry/{slug}`

6.4 Stablecoin Compliance

MiCA Classification Engine (105+ Stablecoins)

`Coverage: USDC, EURC, RLUSD, USDT, DAI · Update: On-demand (5-min cache)`

Configurable policy classification based on EU regulatory register data (ECB, ESMA CASP Register, NY DFS). Returns ACCEPTED/REJECTED status with machine-readable reason codes and configurable policy modes (strict, moderate, relaxed).

Endpoint: `GET /v3/stablecoin/mica/{symbol}`

CCI Score (Crypto Compliance Index)

`Scale: 0-100 with letter grades (A+ to F)`

Composite regulatory compliance score. Weighted methodology: MiCA status (30%), reserve transparency (25%), jurisdiction risk (20%), audit frequency (15%), operational history (10%).

Endpoints: `GET /v3/cci/{symbol}` · `GET /v3/cci/ranking`

6.5 Operational Resilience Tools

Circuit Breaker Detection

`Triggers: Peg deviation, volume anomaly, liquidity drop, oracle failure`

Automated halt detection for DORA operational resilience. Returns ACTIVE/TRIGGERED status with severity level and signed Evidence Pack.

Endpoint: `GET /v3/circuit-breaker/status`

ISO 20022 Payment Validation

`Engine: xmllint (libxml2) · Supported: pain.001.001.09`

XML payment message validation against official ISO 20022 XSD schemas. Returns Evidence Pack with validation decision, error details, and SHA-256 hash.

Endpoint: `POST /v3/iso20022/validate`

6.6 Stablecoin Peg Monitor (105+ Tokens)

Real-Time Peg Deviation Tracking

`Coverage: 105+ stablecoins · Update: Real-time · Source: Multi-exchange aggregation`

Continuous peg health monitoring across 105+ stablecoins. Tracks deviation from peg, trading volume anomalies, and liquidity depth. Returns severity classification

(STABLE / WARNING / CRITICAL / DEPEG) with configurable ale
monitoring.

Endpoints: `GET /v3/stablecoin/mica/{symbol}` · `GET /api/v1/feeds/stablecoin` · `GET /v1/peg/status/{symbol}`

6.7 Significant Issuer Detection (Art. 44)

MiCA Art. 44 Classification Engine

`Criteria: €5B market cap, 10M holders, 2.5M daily transactions`

Automated screening against MiCA Art. 44 significant issuer thresholds. Monitors market capitalization, holder count, and transaction volume to detect when stablecoins cross regulatory significance boundaries. Returns SIGNIFICANT / NON-SIGNIFICANT classification with evidence trail.

Endpoint: `GET /v1/mica/significant-issuer/{symbol}`

6.8 Reserve Drift Monitor (Art. 25)

Reserve Composition Deviation Detection

`Monitoring: Continuous · Threshold: Configurable drift tolerance`

Tracks reserve asset composition changes over time. Detects when reserve backing deviates from declared composition — critical for MiCA Art. 25 compliance (reserve of assets requirements). Flags unauthorized asset substitutions, concentration shifts, and quality downgrades.

Endpoint: `GET /v1/mica/reserve-drift/{symbol}`

6.9 Interest Prohibition Scanner (Art. 23/52)

MiCA Art. 23 & 52 Yield Detection

`Scope: All monitored stablecoins · Regulation: EMT Art. 23, ART Art. 52`

Scans for prohibited interest or yield mechanisms on e-money tokens (EMT) and asset-referenced tokens (ART). MiCA explicitly prohibits granting holders. This scanner detects staking yields, rebasing mechanisms, and distribution schemes that could violate Art. 23/52.

Endpoint: `GET /v1/mica/interest-scan/{symbol}`

6.10 Document Compliance Monitor (Art. 29/30/55)

White Paper & Disclosure Verification

Articles: Art. 29 (EMT white paper), Art. 30 (marketing), Art. 55 (ART white paper)

Monitors whether token issuers maintain compliant white papers and marketing communications as required by MiCA. Checks for mandatory disclosure elements, publication status, and update frequency. Returns compliance status with specific article references for gap remediation.

Endpoint: `GET /v1/mica/document-compliance/{symbol}`

6.11 ESMA Register Mirror

EU Regulatory Register API

Source: ESMA · Update: Daily sync

Machine-readable mirror of the ESMA register for authorized CASPs and licensed token issuers. Enables automated verification of regulatory status against the official EU register. Cross-references with internal MiCA classification for comprehensive compliance checks.

Endpoint: `GET /v1/esma/register` · `GET /v1/esma/register/{entity}`

7. MODULE 2 — Carbon & ESG Context

Module 2 provides per-chain carbon footprint data and sustainability indicators with ISO 14040 methodology. Designed for MiCA Art. 66 sustainability disclosures and CSRD/ESRS reporting requirements.

7.1 Chain-Level Carbon Scoring

Carbon Footprint Feed

`Update: Daily · Coverage: 50+ blockchain networks · Source: CCRI, EMBER, Climatiq`

Blockchain energy and emissions data: carbon per transaction, energy per transaction, consensus mechanism classification, and green score (0–100). Confidence scoring reflects source coverage and data freshness.

Endpoints: `GET /api/v1/feeds/carbon/chains` · `GET /api/v1/feeds/carbon/{chain}`

7.2 Data Provenance

VeChain ToolChain · ISO 14040/14044

`Methodology: ISO 14040 Life Cycle Assessment framework`

Carbon data follows ISO 14040/14044 Life Cycle Assessment methodology. Source provenance is documented per network, with cross-validation against multiple emission factor databases.

7.3 CSRD-Ready Output

ESG Scores for Portfolio Reporting

`Frameworks: CSRD/ESRS, MiCA Art. 66`

ESG scores integrated directly into RWA risk reports via the `.esg_carbon` field. Designed for inclusion in CSRD sustainability reports and MiCA Art. 66 CASP disclosures.

Endpoint: `GET /v1/rwa/esg/{slug}`

7.4 Grid Intensity

Regional Electricity Carbon Data

`Update: 30 min · Source: UK Carbon Intensity API, EMBER, Climatiq`

Regional electricity carbon intensity data for energy-aware applications and validator location analysis.

Endpoint: `GET /api/v1/grid/intensity`

8. MODULE 3 — DORA Compliance

Module 3 provides evidence infrastructure for the Digital Operational Resilience Act (EU 2022/2554). DORA requires financial entities to maintain ICT risk management frameworks, report incidents, test resilience, and manage third-party ICT risks. FeedOracle delivers machine-readable evidence artifacts for these requirements.

Regulatory context: DORA applies from January 17, 2025 to all EU-regulated financial entities including banks, insurers, investment firms, and their critical ICT third-party service providers. German insurance companies are actively building DORA compliance teams.

8.1 ICT Incident Reporting

Structured Incident Evidence Packs

`Standard: DORA Art. 19 · Format: Machine-readable JSON with EPM wrapping`

Generates structured incident report artifacts for major ICT-related incidents as required by DORA Art. 19. Captures incident classification, impact assessment, timeline, root cause analysis, and remediation steps — all wrapped in signed Evidence Packs for regulatory submission.

Endpoint: `GET /v1/dora/incident-report`

8.2 Third-Party Vendor Risk

ICT Third-Party Risk Assessment

`Standard: DORA Art. 28-30 · Scope: Critical ICT service providers`

Risk assessment framework for ICT third-party service providers. Evaluates concentration risk, exit strategies, subprocessor chains, data residency, and service level monitoring — aligned with DORA Art. 28-30 requirements for managing ICT third-party risk.

Endpoint: `GET /v1/dora/vendor-risk`

8.3 Business Continuity Evidence

Operational Resilience Documentation

`Standard: DORA Art. 11-12 · Output: Signed evidence artifacts`

Generates business continuity and disaster recovery evidence artifacts. Documents RPO/RTO targets, backup verification, failover testing results, and recovery procedures — structured for DORA Art. 11-12 ICT business continuity management requirements.

Endpoint: `GET /v1/dora/business-continuity`

9. MODULE 4 — CSRD/ESRS Reporting

Module 4 provides 5 dedicated APIs for Corporate Sustainability Reporting Directive (CSRD) requirements under the European Sustainability Reporting Standards (ESRS). Designed for financial entities reporting on digital asset portfolios and blockchain infrastructure sustainability.

9.1 EU Taxonomy Alignment

Activity Classification & Alignment Scoring

`Framework: EU Taxonomy Regulation (2020/852) · ESRS E1-E5`

Classifies blockchain and RWA protocol activities against the EU Taxonomy. Returns alignment scores for climate mitigation, climate adaptation, and do-no-significant-harm (DNSH) criteria.

Endpoint: `GET /v1/csrd/taxonomy`

9.2 Materiality Assessment

Double Materiality Analysis

`Standard: ESRS 1 §§ 37-58 · Output: Impact & financial materiality scores`

Provides double materiality assessment data for digital asset activities: impact materiality (effects on people and environment) and financial materiality (sustainability risks to the entity). Structured for ESRS disclosure requirements.

Endpoint: `GET /v1/csrd/materiality`

9.3 Emissions Data

Scope 1/2/3 Emissions for Blockchain Infrastructure

`Standard: ESRS E1 · Sources: CCRI, EMBER, Climatiq`

Chain-level and protocol-level greenhouse gas emissions data. Provides Scope 1 (direct), Scope 2 (electricity), and Scope 3 (value chain) emissions estimates for blockchain infrastructure — formatted for CSRD reporting templates.

Endpoint: `GET /v1/csrd/emissions`

9.4 Social Metrics

Workforce & Community Impact

`Standard: ESRS S1-S4`

Social sustainability indicators for RWA protocol assessment: workforce diversity, community impact, human rights due diligence, and consumer protection metrics. Complements environmental data for comprehensive ESG reporting.

Endpoint: `GET /v1/csrd/social`

9.5 Governance

Governance & Risk Management

`Standard: ESRS G1 · Scope: Protocol & issuer governance`

Governance indicators for RWA protocols and token issuers: board composition, risk management frameworks, compliance structures, audit mechanisms, and whistleblower protections. Key input for CSRD governance disclosures.

Endpoint: `GET /v1/csrd/governance`

10. MCP Server & Olas Mech — AI Agent Access

FeedOracle provides a Model Context Protocol (MCP) server with **18 compliance tools** for AI agent integration. The MCP server enables Claude Desktop, Cursor, and any MCP-compatible client to access FeedOracle's evidence infrastructure programmatically — with every response cryptographically signed.

Transport

The MCP server supports two transport protocols: Server-Sent Events (SSE) at `https://feedoracle.io/mcp/sse` and Streamable HTTP. Both provide real-time, bidirectional communication for agent workflows.

TOOL	DESCRIPTION
compliance_preflight	Pre-trade regulatory check — PASS/WARN/BLOCK with reason codes
mica_status	MiCA compliance status for any stablecoin
evidence_profile	Full evidence profile for any RWA protocol
custody_risk	Custody provider risk assessment
market_liquidity	DEX liquidity depth analysis (GeckoTerminal)
evidence_leaderboard	Protocol ranking across 61 RWA protocols & 105+ stablecoins
rlusd_integrity	RLUSD reserve verification with XRPL anchoring
macro_risk	Macro economic risk indicators (FRED/ECB)
peg_deviation	Real-time peg health for any stablecoin
significant_issuer	MiCA Art. 44 significant issuer classification
interest_check	MiCA Art. 23/52 interest prohibition scan
document_compliance	MiCA Art. 29/30/55 white paper verification
reserve_quality	MiCA Art. 25/53 reserve quality assessment
mica_full_pack	Complete MiCA compliance pack for any token
mica_market_overview	Market-wide MiCA compliance overview
peg_history	Historical peg deviation data
generate_report	Generate signed PDF evidence reports
ping	Server health check

Olas Mech Marketplace

FeedOracle is live on the **Olas Mech marketplace** (Gnosis Chain) with 8 tools available for autonomous agent-to-agent interaction. Service 2670 has processed

Discovery

AI agents discover FeedOracle via: `/llms.txt` for LLM-native discovery, OpenAPI 3.0 spec at `/docs/rwa-openapi.json`, and the MCP server's built-in tool listing. All three discovery mechanisms are maintained and synchronized.

11. Architecture

FeedOracle operates as a layered data infrastructure:

```
Layer 6: AGENT ACCESS     MCP Server (18 tools), Olas Mech (Gnosis), llms.txt discovery
Layer 5: EVIDENCE         ECDSA Signatures, Evidence Packs, Multi-Chain Anchoring
Layer 4: COMPLIANCE       MiCA (105+ stablecoins), DORA, CSRD/ESRS, ISO 20022
Layer 3: API GATEWAY      48+ services, REST endpoints, authentication, rate limiting, OpenAPI
Layer 2: PROCESSING       Normalization, quality scoring, confidence calculation, risk aggrega
Layer 1: DATA SOURCES     Blockchain RPCs, CCRI, DeFiLlama, GeckoTerminal, FRED, ECB, ESMA, An
```

The architecture maps to the product modules:

LAYER	CORE (RWA RISK)	MOD 1 (MICA)	MOD 2 (CARBON/ ESG)	MOD 3 (DORA)	MOD 4 (CSRD)
Agent	MCP Server (18 tools) · Olas Mech (Gnosis, 8 tools) · llms.txt · OpenAPI 3.0				
Evidence	ECDSA + SHA-256 + JWKS	Compliance EPMs	Sustainability EPMs	Incident EPMs	Reporting EPMs
Processing	9-vector scoring, anomaly detection	105+ stablecoins, Art. 44, reserve drift, CCI	Carbon normalization, green scoring	ICT risk assessment, vendor scoring	Double materiality, taxonomy alignment
Data Sources	DeFiLlama, FRED, Ankr, GeckoTerminal	ECB, ESMA, OFAC, NY DFS	CCRI, EMBER, Climatiq	Internal + client data	EMBER, CCRI, Climatiq, World Bank

API Specification

All endpoints are documented in OpenAPI 3.0 format with Swa

readable discovery via llms.txt for AI agent integration.

12. Attestation & Evidence

Disclosure Attestation Protocol (DAP)

DAP creates cryptographic proof of data delivery. The protocol hashes API response payloads with SHA-256, aggregates hashes into Merkle trees, and anchors roots to public blockchains.

How It Works

1. **Hash:** API response payload hashed with SHA-256
2. **Sign:** ECDSA signature (ES256K) with JWKS-discoverable public key
3. **Aggregate:** Hashes combined into Merkle trees (batched)
4. **Anchor:** Hash anchored on XRPL (memo field). Gnosis Chain live via Olas Service 2670.
5. **Verify:** Anyone can verify delivery timestamp via block explorer or API

What Gets Hashed

INCLUDED IN HASH	EXCLUDED FROM HASH
API response body (JSON)	HTTP headers
Timestamp (ISO 8601)	Client IP address
Endpoint path	API key (hashed separately)
Schema version	Request parameters

Scope of Proof

DAP proves that specific data was delivered via API at or before the anchored block timestamp, and that post-delivery modification becomes detectable via hash mismatch. DAP is a delivery evidence mechanism — it does not verify upstream data correctness or constitute regulatory approval.

MODE	FREQUENCY	
Anchoring Schedule		
Daily Batch	Once per 24h	All tiers
Hourly Batch	Once per hour	Enterprise
Event-Driven	On significant data change	Enterprise

Evidence Pack Manifest (EPM v1.0)

EPM extends DAP with a standardized manifest schema using DSSE-style envelopes and RFC 8785 deterministic hashing. Supports jurisdiction-aware metadata (EU/UK/US/Global). Every Evidence Pack contains: the signed data payload, ECDSA signature (ES256K), timestamp, schema version, source attribution, and Merkle proof. Public keys are discoverable via JWKS endpoint.

DAP API Endpoints

ENDPOINT	METHOD	DESCRIPTION
/api/v2/attestation/test	GET	Integrity test on all sources
/api/v2/attestation/sources	GET	List attested sources and TLS policies
/api/v2/attestation/anchor/latest	GET	Blockchain anchor status (XRPL)
/api/v2/attestation/merkle	GET	Current Merkle root
/api/v2/attestation/verify/{hash}	GET	Verify payload hash
/api/v1/epm/verify	POST	Verify DSSE-wrapped EPM manifest

Pipeline

```
Sources → Ingestion → Validation → Normalization → Quality Scoring → API → DAP
          (scheduled)  (schema)    (units/format)   (confidence)     (REST) (anchor)
```

Quality Gates

GATE	CHECK	ON FAILURE
Schema Validation	Response matches expected structure	Reject, log, use fallback
Freshness Check	Timestamp within threshold	Flag as stale, reduce confidence
Range Validation	Values within expected bounds	Flag anomaly, manual review
Cross-Validation	Compare multiple sources	Use median, flag divergence

Confidence Scoring

Every data point includes a confidence score (0.0–1.0) reflecting source availability, data freshness, and cross-validation status. Confidence scores are heuristic indicators — not statistical confidence intervals.

Staleness Handling

When primary sources are unavailable, the system attempts configured secondary sources. If all sources are unavailable, the API returns the last known value with a `stale: true` flag and reduced confidence. The staleness threshold is configurable per feed (default: 2× normal update interval).

Security Controls

Operational controls informed by ISO/IEC 27001:2022 principles:

CONTROL AREA	IMPLEMENTATION
Access Control	API key authentication (X-API-Key header), tiered rate limits
Cryptography	ECDSA ES256K signing, SHA-256 hashing, TLS 1.2+ enforced
Network Security	HSTS, CSP headers, firewall, Cloudflare DDoS protection
Backup	Daily encrypted, cross-server sync within EU
Logging	Request IDs, structured access logs, audit trail
Key Management	ECDSA key rotation, JWKS public key discovery

Service Level Objectives

METRIC	TARGET	MEASUREMENT
API Availability	99.5%	Monthly uptime
Response Time (p95)	<500ms	95th percentile latency
Data Freshness	≤15 minutes	Real-time feeds
Attestation Anchor	≤24 hours	Time to on-chain

Data Residency

COMPONENT	LOCATION	NOTES
Primary Infrastructure	Germany (netcup DE)	API servers, databases
Backup Storage	EU	Encrypted, cross-server sync

Blockchain Anchors	XRPL (live), Gnosis (live via Olas Mech)	Public blockchains

Recovery Targets

METRIC	TARGET
RPO (Recovery Point Objective)	≤1 hour
RTO (Recovery Time Objective)	≤2 hours

Subprocessors

SUBPROCESSOR	FUNCTION	LOCATION
netcup GmbH	Infrastructure hosting	Germany
Cloudflare Inc.	CDN, DDoS protection, DNS	US/EU (edge)
XRPL Ledger	Blockchain anchoring	Decentralized
Ripple (XRPL)	Blockchain anchoring	Decentralized

15. Target Users

Banks & Insurers

Portfolio risk assessment for RWA allocations. DORA-supporting evidence packs for third-party vendor risk documentation. Signed evidence artifacts for audit trails.

Asset Managers

Due diligence on tokenized funds. Yield spread analysis vs. T-Bill benchmarks. Smart contract risk signals. ESG/sustainability data for portfolio reporting.

Exchanges & CASPs

MiCA Art. 66 sustainability disclosures for listed crypto-assets

classification and monitoring. Structured data for regulatory reporting ahead of the June 2026 CASP transition deadline.

DeFi Protocols & DAOs

On-chain risk feeds for RWA integrations. DEX liquidity monitoring. Protocol-level risk scoring for governance decisions. Chainlink Functions integration for smart contract access.

RegTech Platforms

White-label compliance modules with API-first integration. OpenAPI spec, versioned schemas, bulk access for platform integration.

AI Agents & Autonomous Systems

Machine-readable API outputs with llms.txt discovery. Pay-per-call access model. DAP enables programmatic verification without human intervention.

16. Competitive Landscape

CATEGORY	FOCUS	EXAMPLES
Decentralized Oracles	DeFi price feeds, on-chain data delivery	Chainlink, Pyth, Redstone
Blockchain Indexers	Query layer for on-chain data	The Graph, Goldsky
Research & Analytics	Market intelligence, reporting	Messari, Dune, Nansen
Carbon Ratings	Sustainability assessments	CCRI, Digiconomist
AML/KYT	Transaction monitoring, wallet screening	Chainalysis, Elliptic, TRM Labs
AI Agent Tooling	MCP servers, agent marketplaces	

Evidence Infrastructure	Regulatory verification + signed evidence + risk scoring + AI agent access	FeedOracle

Differentiation

- **Evidence-first:** Every API response is ECDSA-signed and on-chain anchored — not an optional add-on
- **CORE + Modules:** One risk engine with dedicated compliance (MiCA) and sustainability (ESG) modules
- **Configurable outputs:** Machine-readable policy signals with reason codes, not subjective scores
- **Multi-vertical:** MiCA, DORA, ISO 20022, Carbon/ESG — one Evidence Pack framework
- **Enterprise documentation:** Subprocessor register, incident procedures, procurement pack, exit strategy
- **AI-native:** MCP server (18 tools) + Olas Mech marketplace — compliance tools accessible to autonomous agents, not just human analysts

17. Commercials

Pricing

TIER	PRICE	API CALLS	EVIDENCE PACKS
Free	€0/mo	100/day	–
Developer	€49/mo	5,000/day	50/mo
Professional	€299/mo	50,000/day	500/mo
Enterprise	Custom	Custom	Custom

Payment: Stripe (card) and XRPL crypto payments accepted for all paid tiers.

Evidence Packs are request-based: each API call that generates a Pack counts as one verification. API calls without Evidence are not counted against the verification limit.

Enterprise Package

- Custom SLA negotiation
- DORA Support Pack (ICT third-party risk documentation)
- Dedicated account manager
- Custom integration support and priority incident response
- Historical data access (Data Vault)

18. Roadmap

> **Forward-looking statement:** This roadmap contains planned initiatives. Actual results may differ. No commitment to delivery dates, features, or timelines.

Delivered (Q1 2026)

INITIATIVE	STATUS
RWA Risk Oracle — 61+ protocols, 9 risk vectors, 5 data sources	Live
MiCA Regulatory Evidence module (legal state, jurisdiction, registry)	Live
Carbon & ESG module (50+ networks, ISO 14040)	Live
Macro Economic Oracle (FRED + ECB enrichment)	Live
XRPL Anchoring	Live
Evidence Pack System with ECDSA signing + JWKS	Live
MiCA Stablecoin Classification (105+ stablecoins)	Live
CCI Score Engine (compliance ranking)	Live
ISO 20022 Payment Validation	Live
Circuit Breaker Detection (DORA resilience)	Live

Interactive Enterprise Demos (5 verticals)	
MiCA Deep Compliance: Significant Issuer (Art. 44), Reserve Drift (Art. 25), Interest Scanner (Art. 23/52), Document Compliance (Art. 29/30/55), ESMA Register	Live
DORA Compliance Module (incident reporting, vendor risk, business continuity)	Live
CSRD/ESRS Module (5 APIs: taxonomy, materiality, emissions, social, governance)	Live
MCP Server (18 tools, SSE + Streamable HTTP)	Live
Olas Mech marketplace (Gnosis, 8 tools, 133+ deliveries)	Live
Stablecoin Peg Monitor (105+ tokens, real-time)	Live
Chainlink Functions integration (Polygon, Contract 0xd509...3EE)	Live
L2 Intelligence APIs (7 chains)	Live
Verified Reports System (5 types: RWA Risk, MiCA, DORA, Macro, CSRD) with PDF generation, XRPL-anchored proof panel	Live
Payment Infrastructure — Stripe + USDC (Polygon), 4 tiers (Free / Starter $99 / Pro $299 / Enterprise)	Live
Agent-to-Agent (A2A) Monetization — Pay-per-Call API (9 feeds, USDC on Polygon) + Olas Mech (0.01 xDAI/request, Gnosis)	Live
Report Verification Infrastructure — public /verify endpoints with SHA-256 + ECDSA signature validation	Live
Trust Center & Enterprise Procurement Pack (12 sections: security, SLOs, subprocessors, vulnerability disclosure, compliance mapping)	Live
Public Status Page — Uptime Kuma with 37 monitors across 8 service groups	Live
CSRD/ESRS Data API — chain footprint, ESRS E1, EU energy mix, EU ETS pricing	Live

In Progress (Q1–Q2 2026)

INITIATIVE	
Multi-chain Evidence Anchoring — XRPL (live), Polygon (contract deployed), Avalanche & Flare (grant applications submitted)	In Progress
SOC 2 Type II — Trust Center live, compliance framework mapping complete, security controls documented, SLO evidence via Uptime Kuma (37 monitors). Pre-audit documentation ready; formal audit pending funding	Audit-ready
Chainlink BUILD program participation	Application submitted
Avalanche infraBUIDL() grant — C-Chain deployment, RWA Risk Oracle, Evergreen Subnet integration	Application submitted
Flare Network grant — FTSOv2 Feed Value Provider, FDC compliance attestations, FAssets risk layer	Application ready
CSRD/ESRS template library — structured report templates for ESRS E1 disclosures	Data API live, templates in development

Planned (Subject to Change)

INITIATIVE	PRIORITY
ISO 20022 expansion (pacs.008, camt.053)	Medium
WebSocket real-time feeds (SSE + Streamable HTTP already live via MCP)	Medium
XRPL Grants program application (Spring 2026)	High
Avalanche Evergreen Subnet integration for institutional evidence delivery	Medium
Flare FTSOv2 Feed Value Provider for compliance/risk data feeds	Medium
Flare Data Connector (FDC) attestations for compliance events	Medium

Resources

Documentation	feedoracle.io/docs
API Reference	Full API Ref (190+ Endpoints)
Trust & Security	Trust Documentation
System Status	Status Page
Enterprise	Enterprise Overview
Interactive Demos	RWA · Insurance · Carbon · Stablecoin · Payments

20. Legal & Disclaimers

FeedOracle provides data infrastructure and verifiable evidence artifacts. The platform does not provide financial, legal, or compliance advice. Compliance decisions remain with the institution and its qualified advisors.

Regulatory Sources

Regulatory timelines and classifications referenced in this document are based on the following official sources:

- **MiCA:** Regulation (EU) 2023/1114 — EUR-Lex. Stablecoin provisions (Title III/IV) in force since 30 June 2024. CASP transitional period ends 1 July 2026 per Art. 143(3).
- **DORA:** Regulation (EU) 2022/2554 — EUR-Lex. Applicable since 17 January 2025.
- **CSRD:** Directive (EU) 2022/2464 — EUR-Lex. ESRS delegated acts applicable from 1 January 2024.
- **ESMA CASP Register:** esma.europa.eu
- **BaFin MiCA Guidance:** bafin.de

Forward-Looking Statements

This document contains forward-looking statements regarding roadmap items, and business strategy. Actual results may differ materially. No commitment to specific delivery dates, features, or timelines is expressed or implied.

No Endorsement

FeedOracle is an independent infrastructure provider. References to blockchain networks (XRPL, Polygon, Gnosis, Chainlink), regulatory bodies (ESMA, BaFin, ECB), or data sources (FRED, DeFiLlama) do not imply partnership, endorsement, or affiliation unless explicitly stated.

21. Glossary

A2A
Agent-to-Agent — automated interaction between AI/autonomous systems

CASP
Crypto-Asset Service Provider under MiCA regulation

CCI
Crypto Compliance Index — composite regulatory compliance score (0–100)

CSRD
Corporate Sustainability Reporting Directive (EU)

DAP
Disclosure Attestation Protocol — cryptographic proof of data delivery

DORA
Digital Operational Resilience Act (EU)

DSSE
Dead Simple Signing Envelope — standardized signing format

ECDSA
Elliptic Curve Digital Signature Algorithm (ES256K)

EPM
Evidence Pack Manifest — standardized signed evidence schema

ESRS
European Sustainability Reporting Standards

FRED

Federal Reserve Economic Data — macro economic data source

HHI
Herfindahl-Hirschman Index — concentration measurement

JWKS
JSON Web Key Set — public key discovery endpoint

MCP
Model Context Protocol — open standard for AI agent tool integration (Anthropic)

Mech
Olas Mech — decentralized AI agent marketplace on Gnosis Chain

MiCA
Markets in Crypto-Assets Regulation (EU) — stablecoin rules in force since June 2024, CASP transition ends June 2026

RPO
Recovery Point Objective — maximum acceptable data loss

RTO
Recovery Time Objective — maximum acceptable downtime

RWA
Real World Assets — tokenized traditional financial instruments

SLA
Service Level Agreement — contractual commitment

SLO
Service Level Objective — target performance metric

TVL
Total Value Locked — aggregate value deposited in a protocol