USDPROP Technical Architecture

Technical due diligence package for CTO review, security review, architecture review and fund technical diligence. This document summarizes the deployed architecture, contracts, roles, upgrade model, identity model, compliance engine, treasury controls, deployment records and integration references.

Technical Reference

Parameter	Current value
Network	Polygon mainnet, chainId 137
Token standard	ERC-3643 (T-REX protocol)
Identity	ONCHAINID, ERC-734 / ERC-735 identity and claim model
Proxy pattern	UUPS, OpenZeppelin upgradeable pattern for core upgradeable contracts
Payment token	USDC native Polygon, 0x3c499c542cEF5E3811e1192ce70d8cC03d5c3359
Treasury	Safe multisig, 2/3 threshold in current deployment artifact
Compliance	Reg D 506(c), Reg S and EU MiFID II operational support model
Tooling	Hardhat, ethers.js, OpenZeppelin

Core Standards & Dependencies

Component	Use
ERC-3643	Permissioned Security Token Standard
ONCHAINID	Identity & Claims Framework
Polygon	Settlement Network
USDC	Settlement Asset
Safe	Treasury Governance

Contract Inventory

Deployed contracts, responsibilities and upgrade status.

Contract	Category	Standard	Upgradeable	Address
USDPROP Token	Issuance / ownership record	ERC-3643	Yes	0x6F6c5Ab2865E028beDFEbabD86E046D73EAC5826
IdentityRegistry	Identity registry	ONCHAINID / ERC-734 / ERC-735	Yes	0x82e04Ac5abC1c6979781aeB2ACa5133B59f86bac
ModularCompliance	Transfer compliance engine	T-REX ModularCompliance	Yes	0x42a133b07c53FEb1043Ac84481993ceec72D1294
USDPROPComplianceModule	Custom compliance module	Compliance module	Review	0x6A7863dF05D06956bfE8B7650f2c2983e214bDcc
ClaimIssuer	Claim attestation issuer	ONCHAINID ClaimIssuer	No	0x656B7DDFf86ce7aBE9E86A8bf97642d55B95a61a
InvestmentManager	Subscription execution	EIP-712 + USDC settlement	Yes	0xe901ef0395850A217b19F2cc0819527ae4D2949f

Contract	Category	Standard	Upgradeable	Address
NAVOracle	NAV reference	Oracle adapter	Yes	0x356B60F2600D0454871F9492a4B90cE750b0F9a9
DividendDistributor	Distribution accounting	Distribution module	Yes	0x26FaD8d74c2Eb3461c94e5CeAC8e8AEb48e6D1D1
Safe Treasury	Treasury control	Safe multisig	Configurable	0xe1f7615962BcFEE1C9992A2c501702130835f92c

Roles & Permissions Matrix

Role	Controls	Criticality
Owner	Contract ownership, role assignment, upgrade/admin handoff and emergency authority depending on contract	Critical
ClaimIssuer	Signs, updates and revokes investor claim topics for KYC, AML, accreditation and jurisdiction status.	Critical
AdminAgent	Operational configuration, parameter changes and administrative workflows authorized by ownership policy.	High
NAVAgent	NAV and accounting references consumed by investment, redemption and distribution workflows.	High
DistributionAgent	Distribution lifecycle preparation, entitlement accounting and settlement operation support.	High
SafeSigner	Approves treasury movements and upgrade execution through the Safe threshold model.	Critical
IdentityAgent	Registers ONCHAINID mappings and wallet-to-identity relationships used by transfer checks.	High
ComplianceAgent	Configures claim topics, trusted issuers, transfer modules, lockups and eligibility restrictions.	Critical

Upgradeability Matrix

Contract	Upgradeable	Pattern
USDPROP Token	Yes	UUPS
IdentityRegistry	Yes	UUPS
ModularCompliance	Yes	UUPS
ClaimIssuer	No	Immutable
InvestmentManager	Yes	UUPS
NAVOracle	Yes	UUPS
DividendDistributor	Yes	UUPS
Safe Treasury	Configurable	Safe Configuration

System Architecture

Investor -> KYC Provider -> ClaimIssuer -> IdentityRegistry -> ERC-3643 Token -> InvestmentManager -> NAVOracle -> DividendDistributor -> Safe Treasury. Off-chain systems collect documents and KYC payloads. On-chain registries store identities, issuers and claim references used by the token compliance layer.

Smart Contract Suite

The deployed suite includes the USDPROP Token, IdentityRegistry, ModularCompliance, USDPROPComplianceModule, ClaimIssuer, InvestmentManager, NAVOracle, DividendDistributor and Safe Treasury. Polygonscan address and source tabs are linked from the technical page.

Upgrade Path

Core upgradeable contracts follow the UUPS pattern. Current upgrade authority is expected to be the Safe Treasury with 2 of 3 threshold approval before execution. New variables must be appended only. Existing storage slots must not be reordered, removed or type-mutated.

Investment Flow

investWithConsent(): investor signs EIP-712 consent, backend verifies wallet and request envelope, InvestmentManager executes the subscription, USDC transfers, restricted ownership units are issued and an event is emitted. Review points: nonce handling, deadline handling, slippage controls and replay protection.

Redemption Flow

redeemWithConsent(): investor signs EIP-712 redemption intent, backend validates eligibility and policy, token burn executes, USDC settlement path runs and redemption events update the audit trail.

Identity and Claims

ONCHAINID identities associate wallet addresses with investor identity contracts and verifiable claims. The IdentityRegistry and trusted ClaimIssuer model support KYC, AML, Accredited Investor, Reg D and Reg S claim topics. Claims can be created, verified, updated and revoked.

Compliance Engine

ERC-3643 transfer validation routes through registry and compliance checks before token balances move. canTransfer() and moduleCheck() enforce investor eligibility, country restrictions, lockups, transfer restrictions and claim requirements.

Treasury Governance

Safe multisig is the treasury control boundary. The current deployment artifact records a 2 of 3 threshold. Formal diligence should review owners, modules, spending policies, recovery plan and signer rotation procedures.

Security Model

Threat model review areas: admin key risk, oracle manipulation, signer compromise, claim issuer compromise, replay attacks and upgrade risk. Mitigations include multisig control, role separation, least privilege, monitoring, nonce/deadline checks, EIP-712 domain binding and documented upgrade review.

Deployment Records

Component	Address	Verification Status
USDPROP Token	0x6F6c5Ab2865E028beDFEbabD86E046D73EAC5826	Pending
IdentityRegistry	0x82e04Ac5abC1c6979781aeB2ACa5133B59f86bac	Pending
ModularCompliance	0x42a133b07c53FEb1043Ac84481993ceec72D1294	Pending
USDPROPComplianceModule	0x6A7863dF05D06956bfE8B7650f2c2983e214bDcc	Pending
ClaimIssuer	0x656B7DDFf86ce7aBE9E86A8bf97642d55B95a61a	Pending
NAVOracle	0x356B60F2600D0454871F9492a4B90cE750b0F9a9	Pending
InvestmentManager	0xe901ef0395850A217b19F2cc0819527ae4D2949f	Pending
DividendDistributor	0x26FaD8d74c2Eb3461c94e5CeAC8e8AEb48e6D1D1	Pending
Safe Treasury	0xe1f7615962BcFEE1C9992A2c501702130835f92c	Pending
USDC	0x3c499c542cEF5E3811e1192ce70d8cC03d5c3359	Verified

ABI and Integration

Area	Reference
Repository structure	contracts/, deploy/, scripts/, test/, docs/, frontend/, backend/
External dependencies	Polygon, USDC, OpenZeppelin, Safe, T-REX, ONCHAINID
ABIs	investor-app/src/contracts/abis.js
Fresh deploy checklist	Polygon RPC, deployer EOA with POL, Safe 2/3, USDC test balance, separate KYC agent EOA
Deploy order	Identity contracts, compliance module, token, NAVOracle + InvestmentManager, DividendDistributor, transfer ownership to Safe

Audit Status

No external audit report is published in this repository at this time. Deployment records and public addresses are available. Formal verification, source matching and role review must be performed per deployment.