USD DWIN (USDW) — Professional White Paper

Technical Architecture • Controls • Evidence Pack • ISO-Aligned Mapping

Document ID: USDW-BSC-AUP-ISO-WP-001 | **Version:** 1.0 | **Classification:** External (Auditor / Chain / Exchange) | **Date:** Feb 2026

Issuer / Operator: Dwin Intertrade Company Limited | **Network:** BNB Smart Chain (BSC) Mainnet, Chain ID 56

Primary Contract (Diamond): 0xEd75AD08f416D4e53e4D45dd5140A4C8b84F39Fb

Explorer (Verified):
https://bscscan.com/address/0xEd75AD08f416D4e53e4D45dd5140A4C8b84F39Fb#code

Document Control & Governance

Document Owner	Dwin Intertrade Company Limited
Prepared For	Independent Auditors, Chain Foundations, Exchanges, Banks/PSPs
Control Objective	Provide audit scope, verifiable facts, control mapping, and evidence packaging
Approval Authority	Governance / Audit Board (operational)
Review Trigger	Any diamondCut upgrade, policy update, PoR policy change, or audit cycle
ISO Positioning	ISO-aligned structure and mapping. Not a certification claim.

Non-certification statement: This paper provides an **ISO-aligned control mapping**; it does **not** claim ISO certification unless issued by an accredited certification body.

Table of Contents (Index)

Main Sections

ISO Annexes

Additional Reference Sections

1) Executive Summary

USD DWIN (USDW) is deployed on BNB Smart Chain using an **EIP-2535 Diamond architecture** with a single canonical address dispatching to modular facets. The deployment comprises **58 contracts**, **57 facets**, and **251 functions**, supporting controlled upgrades, role governance, PoR components, compliance modules, emergency safeguards, and integration registries as enumerated in the deployment output provided by management. (On-chain verification is provided by BscScan link above.)

This document is prepared for **audit and chain submission**, emphasizing:

Verifiable On-Chain Facts

Verifiable on-chain facts and boundaries

Control Objectives

Control objectives and enforcement points

Evidence Packaging

Evidence packaging (ISO-style)

ISO Mappings

ISO mappings across **27001 / 22301 / 37301 / 20022**

2) Purpose & Intended Audience

This document provides a complete technical and controls description of USDW for:

→ Independent smart contract security audit

→ Chain foundation / ecosystem due diligence

→ Exchange technical onboarding

→ Bank/PSP integration security review

→ Compliance and operational assurance review

It is deliberately non-promotional and focuses on:

- On-chain architecture and verifiability
- Access control and governance
- Proof-of-Reserve (PoR) and attestation anchoring
- Operational lifecycle (mint/redeem, reconciliation, incident response)
- ISO-aligned controls mapping and evidence packaging

3) System Identifiers (On-Chain Facts)

3.1 Token Parameters (Operational Configuration)

From deployment initialization logs (management-provided):

name()
USD DWIN

symbol()
USDW

decimals()
18

Domain Separator
Set (EIP-712)

Initial Minted Supply
0.5 USDW to deployer (bootstrap)

3.2 Primary Contract & Deployment Summary

From deployment logs (management-provided):

Diamond Address	0xEd75AD08f416D4e53e4D45dd5140A4C8b84F39Fb
Deployer	0xc557ee55f5DbDAc7128fc4D378111a7D68dEb3d6
Contracts Deployed	**58**
Facets Wired	**57**
Functions	**251**

4) Architecture Overview (EIP-2535 Diamond System)

USDW uses an EIP-2535 Diamond architecture: a single canonical address (the "Diamond") dispatches function selectors to modular facets. This enables:

- Controlled upgradeability (facet replacement/addition)
- Isolation of functional domains
- Patch deployment without token migration
- Unified storage with governed change procedures

4.1 Core Diamond Components (BSC)

Key facets (from deployment list):

01

DiamondCutFacet

Upgrade mechanism

02

DiamondLoupeFacet

Introspection

03

OwnershipFacet

Ownership controls

04

UpgradeTimelockFacet

Delayed upgrades

05

UpgradeabilityCompatFacet

Compatibility & verified upgradeability

5) Functional Domains (Facet Grouping)

Auditor-friendly grouping by control domain (domain boundaries first, then per-facet review).

5.1 Token Core / ERC-20 Surface

- CoreERC20Facet
- PermitFacet

Audit focus: ERC-20 invariants; allowance flows; permit; event correctness; reentrancy; enforcement of restrictions via guards/policies.

5.2 Mint / Burn / Supply Controls

- MintBurnFacet (patched & replaced per management logs)
- RedemptionFacet

Audit focus: privileged mint paths; burn correctness; supply accounting; role gating; PoR/policy coupling.

5.3 Proof-of-Reserve (PoR) & Attestation Anchoring

- PoRMultiChainFacet
- PorFacet
- PorPolicyFacet
- PorSnapshotFacet
- OracleViewFacet
- AIOracleFacet

Evidence approach: The organization maintains a PoR third-party audit pack template describing AUP/attestation deliverables and ISO-aligned evidence packaging. **Note:** The PoR pack includes an example canonical entrypoint on another chain; this paper defines the **BSC canonical contract** for this submission. [[[

1

5.4 Peg / Price / FX Reference Controls

- PegPolicyFacet
- PegReferenceFacet
- PriceLogicFacet
- PriceSourcesFacet
- FXRatesFacet

Audit focus: oracle integrity; safe handling of stale/invalid price; policy constraints.

2

5.5 Governance, Roles & Administrative Actions

- RolesFacet
- RoleAdminActionsFacet
- AdminUtilsFacet
- TreasuryWalletFacet
- GovernanceFacet
- GovernorAdapterFacet
- AuditBoardFacet

Audit focus: least privilege; segregation of duties; timelock enforcement; auditability of admin actions.

3

5.6 Compliance & Policy Enforcement

- ComplianceFacet
- CatalogComplianceFacet
- ISOControlFacet
- KYCAMLFacet
- AuthenticityGuardFacet

A compliance-oriented design reference exists describing KYC/AML gating, blacklist/freeze, pause, supply ≤ reported reserves, attestation oracles, and detailed logs (design reference). [

1

5.7 Emergency Management & Transaction Safeguards

- EmergencyFacet
- TransferGuardFacet (patched & replaced per management logs)
- DexSafeguardFacet
- FeatureFlagsFacet

Audit focus: pause semantics; guard bypass prevention; safe-mode correctness.

2

5.8 Bridge / Cross-Chain / Adapters (Extensible Zone)

- CrossChainRegistryFacet
- CrossChainAdapterFacet
- BridgeCompatFacet
- BridgePluginFacet
- RampBridgePluginFacet
- AdapterRegistryFacet

Audit focus: registry integrity; adapter authorization; plug-in whitelisting; replay protection.

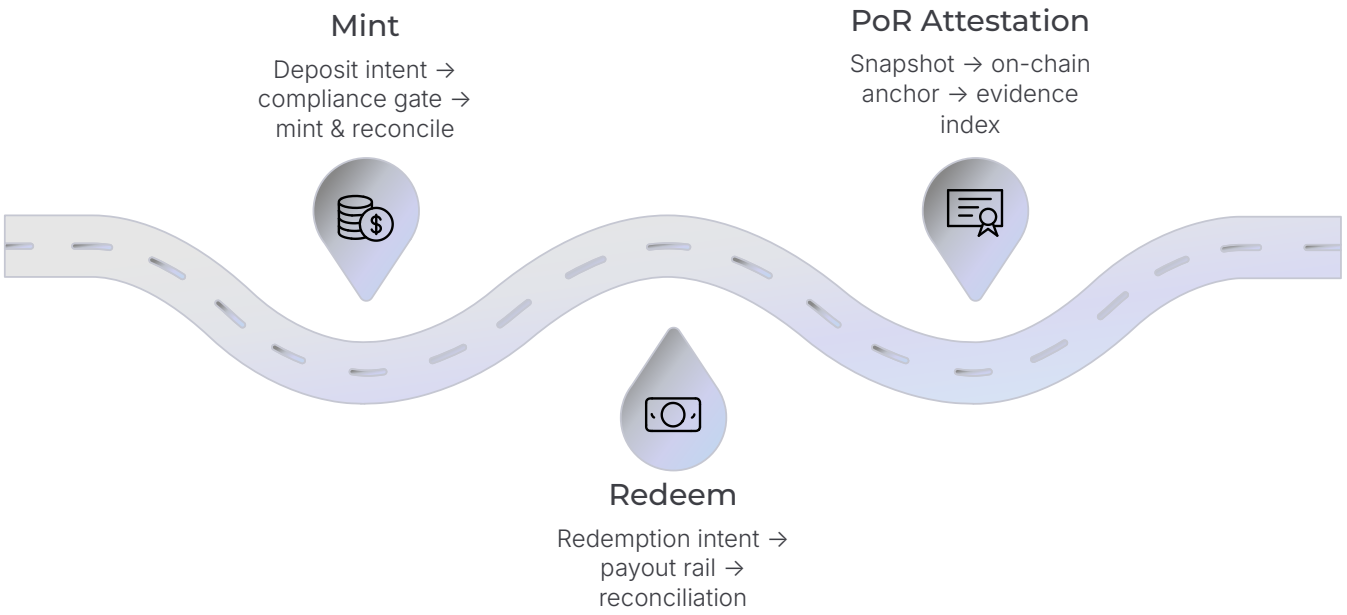
3

5.9 Fiat On/Off-Ramp & Ledger Interfaces

- FiatOnOffRampFacet
- EWalletLedgerFacet
- EWalletFiatLedgerFacet
- GatewayRegistryFacet
- MultiCurrencyReserveFacet

Operational flow references exist in your on/off-ramp architecture document describing deposit intent, bank settlement notification, compliance gates, mint execution, reconciliation, and redeem/burn lifecycle.

6) Operational Lifecycle (Auditor View)



The operational lifecycle covers controlled issuance, controlled burn, and attestation anchoring — each with defined control objectives and evidence requirements.

6.1 Mint (On-Ramp) — Controlled Issuance

Your on/off-ramp architecture describes a flow including: deposit intent → settlement notification → compliance gates → mint → notify → reconcile to bank statements.

Control objective: No mint occurs without:

- authorized role/authority, and
- compliance gate passing, and
- reconciliation capability (bank evidence ↔️ on-chain tx).

6.2 Redeem (Off-Ramp) — Controlled Burn

The architecture reference includes redemption intent creation, payout rail selection, and completion actions that support reconciliation. [

Control objective: No redemption payout without policy adherence and accurate reconciliation evidence.

6.3 Proof-of-Reserve Attestation Anchoring

The PoR audit pack specifies expected audit deliverables: AUP/attestation report, on-chain observation appendix (block numbers/tx hashes), exceptions log, and evidence index mapping procedures to artifacts (ISO-aligned packaging).

Control objective: Attestations and snapshots are verifiable and tamper-evident via on-chain anchoring plus independent evidence.

7) Security Posture & Verification

7.1 Public Verification (Chain Review Requirement)

- Primary contract source is verified on BscScan (link in header).
- Upgradeability compatibility facet verified per management logs.

7.2 Patch Management (Change Evidence)

Management logs indicate:

- patched TransferGuardFacet deployed and wired
- patched MintBurnFacet deployed and wired
- diamondCut (Replace) executed successfully
- instruction to re-run critical security test script

> **Control objective:** Every change is traceable: deploy tx → diamondCut tx → post-change tests → updated manifest.

8) Upgrade & Change Management Controls

Architecture basis: EIP-2535 allows upgrades by swapping facet addresses for selectors.

Required audit checks:

Upgrade Authority

upgrade authority (roles)

Timelock Enforcement

timelock enforcement

Event Logging

event logging

Storage Compatibility

storage compatibility risk

Rollback / Emergency Disable

rollback / emergency disable procedures (if implemented)

9) Governance & Role Controls

Audit goals:

Role Separation

Confirm role separation (admin vs minter vs compliance vs upgrader)

Revocation Flows

Confirm revocation flows

Governance Oversight

Confirm governance / audit board oversight paths

---

10) Compliance Controls (KYC/AML, Policy Catalog)

Compliance modules are designed to support KYC/AML gating, freezing/blacklisting, pause, supply ≤ reserves, and detailed event logs (per design reference). **[# USDW Sta…S complian | Txt]**

---

11) Proof-of-Reserve (PoR) Attestation & Evidence Anchoring

The organization maintains:

A PoR third-party audit pack template (DOCX) and fillable PDF for reviewers, describing scope, expected deliverables, and ISO-aligned evidence packaging.

12) Fiat On/Off-Ramp & Ledger Controls

Operational design reference describes:

On-Ramp

- settlement notification
- compliance gates
- mint
- reconciliation

Off-Ramp

- redeem intent
- payout rails
- reconciliation steps

---

13) Chain / Exchange Technical Checklist (Submission-Ready)

✅ Verified contract on explorer

✅ Canonical entrypoint address (Diamond)

✅ Token metadata initialized (name/symbol/decimals)

✅ Upgrade controls documented (timelock, authorized roles)

✅ Emergency controls documented

✅ Mint/burn authority documented

✅ PoR method documented + auditor AUP pack available

✅ On/off-ramp operational flow documented (if applicable) [[

14) Audit Scope Definition

14.1 In-Scope (BSC Mainnet)

- Diamond contract (canonical entrypoint): `0xEd75AD...39Fb`
- Facets wired (57)
- Role system & admin actions
- Upgrade timelock behavior
- PoR modules, snapshots, policies
- Mint/burn/redemption logic
- Transfer guards, emergency controls
- Compliance/KYCAML enforcement paths
- Registry/adapter boundaries

14.2 Out-of-Scope (Unless Requested)

- Banking partner internal controls (unless ISAE/SOC engagement)
- KYC vendor internals (unless vendor assurance)
- Client application code (unless provided)

15) Evidence Package & Evidence Index

15.1 On-Chain Evidence (Minimum Set)

1. Contract verification link (BscScan)
2. Deployment transactions (deploy + diamondCut + init + domain separator)
3. Loupe output: facets + selectors
4. Role assignment events
5. Upgrade timelock configuration
6. Emergency configuration
7. PoR snapshot txs + anchors
8. Oracle configuration (price sources/policies)

PoR audit pack expects on-chain observation appendix with block/timestamp/tx hashes.

15.2 Off-Chain Evidence (Operational Assurance)

From your architecture reference, evidence commonly includes settlement notifications, reconciliation reports, compliance outputs, incident logs, and policy documents.

15.3 Evidence Index Naming (ISO-aligned packaging)

PoR audit pack describes ISO-aligned evidence packaging and indexing.

Evidence ID format: `USDW-BSC-[DOMAIN]-[NNN]` Domains:

GOV governance, roles, approvals	**UPG** upgrade/timelock	**POR** attestations/snapshots	**MNT** mint/burn/redemption
CMP compliance/KYCAML	**SEC** testing/scanning/IR	**OPS** recon/bank evidence	

16) Risk Register (Audit-oriented)

Risk Area	Description	Expected Evidence / Test
Upgrade Risk	facet replacement introduces new bugs	diamondCut txs + timelock evidence + regression tests
Privileged Access	admin/minter misuse or key compromise	role design, key custody policy, revoke tests
Oracle/Price Risk	stale/incorrect price input	oracle configuration evidence, fail-safe behavior tests
PoR Integrity	attestation mismatch vs supply	PoR snapshots + third-party report + on-chain anchoring
Compliance Risk	sanctions/KYC gaps	KYC/AML policy evidence + enforcement traces
Continuity Risk	inability to respond during incident	emergency playbook + pause tests + upgrade recovery evidence

ISO ANNEXES — Finalized for All Required Standards

ISO Annex A — ISO/IEC 27001 (ISMS) Mapping (Structure + Evidence)

ISO 27001 Annex A (2022) uses **93 controls** grouped into **Organizational, People, Physical, Technological** categories; selection is typically justified in a **Statement of Applicability (SoA)**.

A.1 ISO 27001 Clauses (4–10) — Mapping Template (Auditor-usable)

Clause	Control Objective	USDW Implementation	Reference	Evidence IDs
4	Context	scope, stakeholders, boundaries	Section 2, 14 (scope), registry boundaries	GOV-001...
5	Leadership	security governance & accountability	GovernanceFacet, AuditBoardFacet (existence), doc control	GOV-010...
6	Planning	risk assessment, risk treatment	Risk register (Sec 16), change mgmt (Sec 8)	SEC-020...
7	Support	competence, awareness, doc info	Document Control section + evidence index	OPS-030...
8	Operation	operational controls execution	mint/redeem lifecycle + compliance gates	MNT-040...
9	Performance	monitoring, audit, review	AuditBoard logs + evidence capture	GOV-050...
10	Improvement	corrective action, continual improvement	patch/replace facets + post-tests	UPG-060...

A.2 ISO 27001 Annex A (2022 Themes) — High-Level Mapping

Annex A Theme	What Auditors Expect	USDW Control Points
Organizational (A.5)	policies, supplier, change, incident	Governance + timelock + PoR AUP pack [
People (A.6)	roles, awareness, insider risk	RolesFacet + least privilege evidence
Physical (A.7)	data center, physical access	off-chain domain (OPS evidence, if applicable)
Technological (A.8)	access, logging, crypto, secure dev	verified contracts + upgrade controls + emergency controls

Deliverable expectation: Auditor typically requests your **SoA** (Statement of Applicability) listing chosen Annex A controls and evidence references. ISO 27001 guidance commonly emphasizes SoA as required documentation.

ISO Annex B — ISO 22301 (BCMS) Mapping

ISO 22301 defines requirements for a **Business Continuity Management System**, including planning, implementation, monitoring, review, and improvement.

B.1 ISO 22301 Clause Mapping (Annex SL style)

Clause	BCMS Objective	USDW Mapping	Evidence IDs
4	Context	define BC scope & dependencies — Scope + supplier dependency list (oracle/bank/KYC)	OPS-100…
5	Leadership	leadership commitment — governance document control + approvals	GOV-110…
6	Planning	BIA + risk — BIA/RTO targets for mint/redeem/PoR	OPS-120…
7	Support	resources & comms — incident comms plan + runbooks	OPS-130…
8	Operation	continuity procedures — emergency pause + upgrade recovery process	SEC-140…
9	Performance	exercises & reviews — drill evidence + review minutes	OPS-150…
10	Improvement	corrective actions — post-incident corrective actions	OPS-160…

ISO Annex C — ISO 37301 (Compliance Management System) Mapping

ISO 37301 provides requirements and guidance to establish, implement, evaluate, maintain and improve a compliance management system.

C.1 ISO 37301 Clause Mapping (Auditor-usable)

Clause	CMS Objective	USDW Mapping	Evidence IDs
4	Context	obligations, stakeholder needs — compliance obligations register	CMP-200...
5	Leadership	compliance culture, policy — compliance policy + governance	CMP-210...
6	Planning	compliance risk assessment — compliance risk register	CMP-220...
7	Support	competence, comms, docs — training records + documented info	CMP-230...
8	Operation	controls & procedures — KYC/AML gating design reference	CMP-240...
9	Performance	monitoring, audit — compliance KPIs + internal audits	CMP-250...
10	Improvement	nonconformity, corrective action — remediation records	CMP-260...

ISO Annex D — ISO 20022 Readiness & Messaging Controls

ISO 20022 is a global financial messaging standard using a standardized modeling methodology and repository; it is commonly implemented with **XML message structures** and aims for richer structured data and interoperability.

Your on/off-ramp design explicitly includes bank settlement notifications, reconciliation, and structured bank statement matching (MT940/BAI2/CSV mentioned), which are the typical operational areas where ISO 20022 messaging is applied in banking integrations.

D.1 ISO 20022 Control Objectives for USDW Integrations (No overclaim)

> This annex is written as **readiness / interface control requirements**, not as a claim that ISO 20022 is already implemented on-chain (ISO 20022 is a messaging standard for inter-institution communication).

ISO 20022 Area	Objective	USDW Integration Mapping	Evidence
Data richness	ensure structured remittance & payer data	ledger + gateway registry + reconciliation process OPS-300... [	OPS-300...
Interoperability	standardize messages across partners	message mapping specification for bank partners	OPS-310...
Validation	prevent payment/statement failures	test plan + schema validation logs	SEC-320...
Audit trail	full traceability	evidence index + on-chain tx references	OPS-330...

D.2 ISO 20022 Implementation Guidance References (External)

- ISO 20022 is promoted for richer structured payment data and interoperability (XML-based messaging referenced in industry guidance).
- ISO 20022 repository explains the business model and standardized business concepts used to derive message definitions.

Recommended chain/auditor attachment: "ISO 20022 Message Mapping Specification" (a separate doc) defining the exact message sets used with each bank/PSP partner (pacs/camt categories), plus test evidence and versioning.

Evidence Index, On-Chain Reference Index & References

Evidence Index (Fillable, ISO-Style)

Use the following table template exactly (auditors like this format).

Evidence ID	ISO Ref (A/B/C/D)	Description	Location (URL / file / tx hash)	Owner	Date	SHA-256 Hash

Example ID prefixes: GOV, UPG, POR, MNT, CMP, SEC, OPS (as defined in Section 15.3).

On-Chain Reference Index

Item	Value
Diamond (Canonical)	0xEd75AD08f416D4e53e4D45dd5140A4C8b84F39Fb
Explorer	https://bscscan.com/address/0xEd75AD08f416D4e53e4D45dd5140A4C8b84F39Fb#code
Chain	BNB Smart Chain (56)

References (Internal + External)

Internal references located in your enterprise repository (evidence / templates)

1. **USDW Proof-of-Reserves (PoR) Oracle Independent Third-Party Audit Pack (AUP/Attestation) Template (DOCX)** — includes scope, deliverables, evidence index packaging.
2. **USDW PoR Third-Party Audit Pack (Fillable PDF)** — bank-facing pack with expected deliverables and evidence mapping structure.
3. **README — USDW PoR Audit Package** — describes pack contents and ISO-aligned evidence packaging (informational).
4. **USDW On/Off-Ramp Architecture — DwinPayment × Bank (DOCX/PDF)** — on-ramp/off-ramp steps, reconciliation references.
5. **USDW Stablecoin — MiCA/US compliance-oriented design note (TXT)** — documents compliance gating features and audit-friendly design goals.
6. **Final USDW2028 Architecture Specification (DOCX)** — snippet indicates ISO alignment intent across multiple ISO frameworks (ISOReady statement).

External standards guidance used for ISO annex summaries

1. ISO 27001:2022 Annex A overview and SoA requirement explanation.
2. ISO 22301 official overview: BCMS requirements and purpose.
3. ISO 37301 official overview: compliance management system requirements and guidance.
4. ISO 20022 industry guidance: XML-based structured financial messaging and migration risks.
5. ISO 20022 repository: business model and standardized business concepts.