CERTISYN

Certisyn Security Overview

Architecture, controls, and compliance posture

Document ID	CS-DOC-SEC-002
Version	2.0
Entity	Certisyn, Inc.
Jurisdiction	Delaware, United States
Classification	CONFIDENTIAL

Summary

This document describes the security architecture and compliance posture of the Certisyn platform. The architecture is designed around five invariants: tenant isolation at the database layer, cryptographic sealing of all verification outputs, bounded disclosure by policy, append-only audit ledgers, and a post-quantum migration path for attestation integrity.

Current security posture. Bastion rating AAA+. DMARC p=reject enforced. HSTS, CSP, and permissions-policy headers applied to every public surface. Response signing via HMAC-SHA256. Secrets-at-rest encryption. Zero credential exposure across public endpoints. SOC 2 controls operational; Type II audit in progress.

Tenancy isolation

Every partner, client, and engagement is scoped to a dedicated tenant namespace. Database access is enforced by row-level security policies bound to the authenticated user's tenant membership. A cross-partner read is architecturally impossible: the policy layer rejects the query before the database engine evaluates any row.

Cross-partner data sharing (for example, the anonymised opportunity graph) passes through a dedicated server-side projection function executing under elevated privilege, which is the single architectural ingress into shared state. Identity-bearing fields are suppressed by the projection function before the projection is written to the shared store.

Attestation integrity

Every verification output is cryptographically sealed. The seal references the content hash of the policy artifact under which the output was computed, the full derivation chain entry identifiers, and a timestamp. A reviewer holding the sealed output, the policy artifact, and the evidence records can reproduce the computation byte-for-byte.

Attestation outputs are portable: they do not require ongoing access to the Certisyn platform to be verified by a recipient. The sealed envelope is self-contained — the recipient can inspect the seal, verify the policy artifact hash against a published registry, and validate the derivation chain independently.

Post-quantum readiness

Certisyn's attestation protocol includes a dual-signature architecture supporting FIPS 204 and CNSA 2.0 standards. Attestations issued today include both a classical signature and a post-quantum signature, pre-positioning the platform for the regulatory transition to post-quantum cryptography without retroactive revocation of current attestations.

Bounded disclosure

A Bounded-Disclosure Policy runs at render time on every verification output. For each viewer role, the policy defines the subset of output fields that may be rendered and the subset that must be redacted. A client sees the attestation fields applicable to their engagement; a partner sees their own engagement data and the shared commercial fields; a regulator receives a differently-shaped disclosure appropriate to their mandate. The policy itself is versioned and auditable.

Append-only audit ledger

Every identity reveal, every consent transition, every dispatched agentic action, and every attestation commit is recorded on a cryptographically chained ledger. Ledger entries are immutable by construction: modifying a historic entry would invalidate all subsequent entries. This ledger is the institutional record under which platform operations are auditable after the fact.

Autonomous operations

A significant fleet of autonomous agents observes signals across the platform, reasons across evidence, and prepares action artefacts for human review. Every external action (email, calendar invite, proposal dispatch) is approved by a human before dispatch. Every dispatch is recorded on

the audit ledger, bound to the drafting policy version under which the artefact was composed. Decline and edit signals feed back into the drafting policy as labelled training pairs.

Access controls

Authentication. JWT with HMAC-SHA256, short-lived access tokens, refresh via rotating refresh tokens. Multi-factor authentication available for all partner accounts.

Authorisation. Role-based with row-level policy enforcement at the database layer. Cross-tenant reads architecturally impossible.

Network. TLS 1.3 across all surfaces. HSTS enforced. Certificate pinning on the Certisyn API. All webhook callbacks signed with HMAC-SHA256.

Compliance posture

Delaware C-Corporation. GDPR and CCPA compliant. SOC 2 controls operational with Type II audit in progress. DPA available under mutual NDA. Data Processing Addendum, Privacy Policy, and Terms of Service available on request.

Reporting channels

Security reports: security@certisyn.com. Vulnerability disclosure: responsible disclosure programme under 90-day coordinated disclosure window.

This document is provided for informational purposes only under the requesting party's stated use. It does not constitute a commercial offer or a warranty of specific performance. For commercial engagement terms, contact investor@certisyn.com.