SOC 2 Readiness Summary

Public overview of PasskeyBridge's SOC 2 Type II programme, control coverage, and supporting evidence available under NDA.

DOCUMENT	SOC 2 Readiness Summary v1.0
ISSUED	April 30, 2026
STATUS	Pre-audit readiness • CPA firm engaged • Type I targeted next quarter
CRITERIA	Security, Availability, Confidentiality (TSC 2017, with 2022 points of focus)
AUDIENCE	Enterprise prospects, procurement, vendor security review teams

1. Programme status

PasskeyBridge has initiated a SOC 2 Type II programme covering the Security, Availability, and Confidentiality trust services criteria. Pre-audit readiness work, control mapping, evidence automation, and policy attestation, is in progress with an independent CPA firm. The Type I point-in-time report is targeted for the next quarter, with the Type II observation window beginning immediately afterward. The firm name and observation period will be published on /security once the window opens.

2. Trust services criteria coverage

Criterion	Status	Evidence stream
CC1 Control Environment	Mapped	Org chart, role matrix, code of conduct, board minutes
CC2 Communication & Information	Mapped	Customer comms log, status page, changelog, security memo trail
CC3 Risk Assessment	Mapped	Quarterly risk register, threat model (STRIDE), pentest output
CC4 Monitoring Activities	Operational	Daily codebase sweep, anomaly scanner, canary mesh, function-status metrics
CC5 Control Activities	Operational	Branch protection, SHA-pinned CI, mandatory reviewers, deploy approvals
CC6 Logical & Physical Access	Operational	Multi-tier admin gate, has_role check, breakglass M-of-N, RLS audit
CC7 System Operations	Operational	Live monitoring workflow, status snapshots, incident playbooks
CC8 Change Management	Operational	PR-based deploys, ci.yml gates, bundle/secret/edge checks
CC9 Risk Mitigation	Mapped	Vendor DPAs, sub-processor 30-day notice, Schrems III hashed-signal
A1 Availability	Operational	/status snapshots, multi-region failover, uptime SLOs
C1 Confidentiality	Operational	Zero-PII at edge, AES-256-GCM PBPBV, BLAST tunnels, BYOK

3. Evidence available under NDA

Enterprise prospects executing a mutual NDA receive the full readiness package, which includes:

- Control matrix mapping every TSC criterion to the implementing code, configuration, or runbook.
- CI hardening evidence: ci.yml, live-monitoring.yml, memory-verification.yml workflow definitions and recent run logs.
- Internal pentest suite output (shield-pentest-suite) covering authentication, RLS boundaries, SSRF surfaces, and rate limits.
- Breakglass session logs demonstrating M-of-N approval, time-bounded access, and append-only audit trail.
- DSAR cadence: 1-hour idempotency, cryptographic shredding, sample fulfilment timeline.
- Vendor sub-processor list with executed DPAs and Schrems III hashed-signal architecture diagram.
- Incident response playbooks and 72-hour breach notification runbook (GDPR Article 33).
- Daily codebase sweep aggregating secrets/PII/RLS/dist/bundle/edge/audit/memory checks.

4. Architectural commitments backing the controls

- **Zero-PII at the edge.** Phone numbers and other primary identifiers are SHA-256 hashed at the ingestion boundary. Plaintext is never persisted, logged, or forwarded to AI providers or sub-processors.
- **Tenant isolation.** Every multi-tenant table enforces row-level security keyed on tenant_id. Cross-tenant reads are structurally impossible from the application layer.
- **Bring Your Own Key (BYOK).** Tenant signing keys (P-256 ECDSA for VC issuance) are generated and rotated under the tenant's control.
- **Cryptographic erasure.** The Purpose-Bound PII Vault stores AES-256-GCM ciphertext keyed per tenant. Deleting the key renders the data unrecoverable, satisfying GDPR Article 17 even when backup copies exist.
- **Append-only audit trails.** Breakglass sessions, admin mutations, and DSAR shredding events are written to immutable audit tables.
- **Hybrid post-quantum signatures.** ML-DSA-65 (NIST FIPS 204) co-signs identity assertions alongside classical ECDSA.

5. Out of scope for this summary

This public summary intentionally does not include: the executed CPA letter of engagement, specific control failure remediations, internal infrastructure diagrams, vendor pricing, or anything that could materially aid an attacker. Those artefacts are covered by the full readiness package made available under a mutual NDA.

6. Requesting the full readiness package

Submit a request at **passkeybridge.io/security/soc2-request** with your work email, company, and intended use. Our security team replies within one business day with the NDA and the full evidence package. Direct contact: **security@passkeybridge.io**.
