Vendor Assessment Criteria

Custodial Enterprise Wallet Providers

Solana Developer Platform (SDP)

---

1. Overview

This document defines the assessment criteria for onboarding custodial enterprise wallet providers to the Solana Developer Platform. These providers are listed as available integrations within SDP, enabling institutional developers to access custody infrastructure through a unified API on devnet.

Scope: Custodial enterprise wallets only. This category covers providers that hold private keys and sign transactions on behalf of institutional clients. Wallet-as-a-Service (WaaS) infrastructure providers and self-custodial/embedded wallet solutions are assessed under separate criteria.

Framing: Onboarded providers are presented as *available integrations*, not endorsed or recommended partners. SDP does not assume liability for custodian performance, security, or regulatory standing.

2. Assessment Structure

The assessment uses a two-tier model. Hard Gates are binary pass/fail requirements. Failure on any gate disqualifies the applicant. Scored Criteria are weighted evaluations used to assess fit and prioritize onboarding when multiple applicants are in the pipeline.

Hard Gates (Section 3): All four gates must be passed. Any single failure is disqualifying. No exceptions, no conditional passes.

Scored Criteria (Section 4): Evaluated on a 1-5 scale across three categories. Minimum composite score of 3.0 required to proceed. Scores below 2.0 on any individual criterion trigger a review.

3. Hard Gates (Pass / Fail)

Each gate must be cleared before proceeding to scored evaluation. Applicants that fail any gate are notified with a specific explanation and may reapply when the deficiency is resolved. Assessment scorecard is available here:
SDP_Custodial_Wallet_Scorecard.xlsx.

GATE 1: SOLANA TECHNICAL CAPABILITY

Criterion	Requirement	Evidence Required
Arbitrary Transaction Signing	Must support passing an arbitrary serialized Solana transaction to their signing infrastructure and returning a valid signature. This is the primary signing interface for SDP integration.	Live demonstration on devnet with SDP-provided test transactions
Token-2022 (Token Extensions) Support	Must be able to sign transactions involving Token-2022 program mints. Native platform support for T22 send/receive is preferred but not required at gate level. Must not reject or mishandle T22 transactions.	Successful signing of SDP T22 test suite (provided during sandbox validation)
Solana Account Model	Must correctly handle associated token accounts, rent exemption, and Solana-specific transaction structure (versioned transactions, compute budget instructions).	Demonstrated in devnet integration testing

GATE 2: SECURITY BASELINE

Criterion	Requirement	Evidence Required
Key Management Architecture	Must use MPC, HSM, or equivalent institutional-grade key management. Single-key or browser-based signing is disqualifying. Must document threshold scheme, shard distribution, and key recovery procedures.	Architecture documentation; third-party audit report or SOC 2 Type II covering key management controls
Penetration Testing	Must have completed an external penetration test by a recognized third party within the last 18 months with no unresolved critical findings.	Executive summary of most recent penetration test report
Incident Response	Must have a documented incident response plan. Must not have experienced a security breach resulting in loss of client funds.	Incident response policy document; signed attestation regarding breach history

GATE 3: REGULATORY STANDING

Criterion	Requirement	Evidence Required
Licensing / Registration	Must be licensed or registered as a custodian, trust company, or equivalent in at least one recognized jurisdiction. Money transmitter licenses alone are	Copy of license or registration; jurisdiction and issuing authority identified

GATE 3: REGULATORY STANDING		
	insufficient. Recognized jurisdictions include but are not limited to: USA, EU/EEA (MiCA), UK (FCA), Singapore (MAS), UAE (VARA/ADGM), Japan (FSA).	
AML/KYC Program	Must maintain a documented AML/KYC compliance program appropriate to its jurisdiction and client base.	AML/KYC policy summary (detailed policies available upon request)

GATE 4: OPERATIONAL VIABILITY		
Criterion	**Requirement**	**Evidence Required**
Business Continuity	Must be a funded, operating business with no publicly known insolvency proceedings or regulatory enforcement actions that would materially affect operations.	Self-attestation; SDP team conducts independent verification
Institutional Client Base	Must have at least one live institutional client using their custody product in production. Pre-revenue startups without production deployments are not eligible.	Client reference (name can be withheld; reference call available)

4. Scored Criteria (Weighted Evaluation)

Applicants who pass all four gates are evaluated on the following scored criteria. Each criterion is scored 1-5 by the SDP engineering and partnerships team. The composite score is calculated using the weights below. A minimum composite score of 3.0 is required.

TECHNICAL DEPTH (Weight: 50%)			
Criterion	**What We Evaluate**	**Scoring**	**Weight**
Native T22 Platform Support	Does the custodian's UI/dashboard natively display and support Token-2022 assets (balances, send, receive)? Or is support limited to raw signing only?	1 = raw signing only; 3 = partial UI support; 5 = full native T22 in platform	**15%**
Transaction Policy Engine	Programmable approval workflows: quorum rules, address whitelisting, velocity limits, transaction type restrictions. Does the policy engine handle Solana-specific transaction types correctly? Critical for future SDP policy framework integration.	1 = basic approve/reject; 3 = configurable rules; 5 = fully programmable with Solana-aware policies	**20%**
API Quality & Developer Experience	REST API documentation, SDK availability, webhook support, idempotent operations, error handling, sandbox/testnet environment. Since SDP calls the custodian's signing API directly, reliability and documentation quality directly impact the unified API layer.	1 = minimal docs, no SDK; 3 = documented API with sandbox; 5 = comprehensive SDKs, webhooks, excellent docs	**15%**

SECURITY & COMPLIANCE MATURITY (Weight: 30%)			
Criterion	**What We Evaluate**	**Scoring**	**Weight**
Audit & Certification Depth	SOC 2 Type II, ISO 27001, or equivalent. Type I is a baseline; Type II demonstrates sustained controls. Multiple certifications increase score.	1 = no formal cert; 2 = SOC 2 Type I; 3 = SOC 2 Type II; 5 = Type II + ISO 27001 or equivalent	**15%**
Insurance Coverage	Digital asset insurance (crime, specie, E&O). Coverage limits relative to AUC. Willingness to disclose coverage details.	1 = no insurance; 3 = basic coverage; 5 = comprehensive coverage with disclosed limits	**10%**

SECURITY & COMPLIANCE MATURITY (Weight: 30%)			
Regulatory Breadth	Number and quality of jurisdictions where licensed. Multi-jurisdictional licensing demonstrates broader compliance capability.	1 = single jurisdiction; 3 = 2-3 jurisdictions; 5 = 4+ major jurisdictions	**5%**

OPERATIONAL MATURITY (Weight: 20%)			
Criterion	**What We Evaluate**	**Scoring**	**Weight**
Uptime & Reliability	Published uptime SLA, incident history transparency, status page availability. Willingness to share historical uptime data.	1 = no SLA; 3 = 99.5% SLA with status page; 5 = 99.9%+ SLA with public incident history	**8%**
Institutional Track Record	Number and profile of institutional clients. Assets under custody as a proxy for operational stress-testing. Time in market.	1 = <1 year, few clients; 3 = 2-3 years, multiple institutions; 5 = 4+ years, significant AUC, named references	**7%**
Support & Responsiveness	Dedicated institutional support team, defined SLA for support response times, escalation procedures, integration support quality.	1 = email only, no SLA; 3 = dedicated team with SLA; 5 = 24/7 support with <1hr critical response	**5%**

5. Assessment Process

5.1 Intake

Applicant submits a self-service intake form covering: company overview, regulatory standing, Solana technical capabilities, key management architecture, and client references. SDP team reviews for completeness within 5 business days.

5.2 Gate Evaluation

SDP engineering runs the applicant through the four hard gates. Gate 1 (Technical Capability) is evaluated through a live devnet integration test using the SDP sandbox. The applicant is expected to complete integration independently using SDP documentation, with engineering support available for questions. Gates 2-4 are evaluated through documentation review and verification.

Timeline: Gate evaluation typically completes within 2-3 weeks, depending on applicant responsiveness and integration complexity.

5.3 Scored Evaluation

Applicants who pass all gates are scored by the SDP team (engineering + partnerships). Scores are documented with justification. Composite score must meet the 3.0 minimum threshold.

5.4 Decision & Onboarding

- Pass all gates + composite score 3.0+: Approved for onboarding. Integration listed on SDP devnet.
- Pass all gates + composite score below 3.0: Deferred. Applicant notified of specific areas to improve. May reapply in 6 months.
- Fail any gate: Rejected with specific explanation. May reapply when deficiency is resolved.

6. Ongoing Obligations

Onboarding is not permanent. Listed custodians must maintain the standards that qualified them. The following ongoing requirements apply:

- Annual re-attestation of regulatory standing, insurance coverage, and security certifications.
- Notification to SDP within 5 business days of any material security incident, regulatory action, or change in licensing status.
- Maintenance of devnet integration compatibility. SDP may run periodic integration tests; persistent failures may result in delisting.
- SDP reserves the right to delist a provider at any time if it determines the provider no longer meets the assessment criteria or poses reputational risk to the platform.

7. Scope Limitations & Disclaimers

This assessment evaluates fitness for listing as an available integration on SDP. It does not constitute an endorsement, recommendation, or warranty by the Solana Foundation regarding any custodian's suitability for a specific institution's needs.

Institutions using SDP are responsible for conducting their own due diligence on any custodian they select. The Solana Foundation assumes no liability for the performance, security, regulatory compliance, or business continuity of any listed provider.

All current integrations are on devnet. Criteria for mainnet promotion will be defined separately and may include additional requirements.

Appendix A: Scoring Reference

Score	Definition
5	Excellent. Industry-leading capability. Exceeds requirements with no material gaps.
4	Strong. Meets all requirements with meaningful differentiation in this area.
3	Adequate. Meets the requirement. Functional but not differentiated.
2	Below expectations. Partial capability with notable gaps. Triggers individual criterion review.
1	Deficient. Minimal or no capability in this area.