PARTNER REVIEW / 01 OF 07

The Madiba Standard

Madiba Verify, transaction orchestration, committed liquidity and USDT settlement on Solana.

Partner discussion draft | 25 October 2026 | Version 1.0
This document proposes an implementation and commercial operating model. It does not confirm that a liquidity guarantee, production corridor, service level or partner agreement is already in force.

1. Purpose and intended outcome

Madiba coordinates sender identity and recipient verification through Madiba Verify, followed by Forex/quote, collection, conversion/payout, settlement, reconciliation and all partner fees. SharpSharp.cash is the flagship interface. One master reference links verification decisions, execution and accounting evidence. See the verification layer on pages 6-7.

The target experience is immediate local payout after confirmed collection, supported by a liquidity provider that commits funds before collection. USDT on Solana provides the proposed common partner settlement rail. Settlement and reconciliation are event-driven; completion is recorded only when their agreed evidence requirements are met.

2. What each participant owns

Participant	Proposed responsibility
Madiba / SharpSharp	Customer interface; verification and quote coordination; route selection; master reference; event tracking; reconciliation and fee allocation.
Collection partner	Execute collection; provide authoritative payment status, funding availability and reversal rules; perform its agreed compliance controls.
Liquidity / conversion provider	Issue an executable local-liquidity commitment; lock conversion terms; fund or arrange payout; accept settlement under agreed credit and timing terms.
Payout partner	Validate destination support; execute bank/mobile money delivery; provide definitive delivery or failure status and recovery support.
Settlement / wallet operator	Authorize and execute agreed USDT transfers; manage approved addresses, network costs, signing controls and blockchain evidence.

3. Operating boundary

Madiba's intended role is technology orchestration without custody of customer funds. Financial partners execute the underlying transfers. Contracts must identify who holds funds or tokens at each stage, performs each compliance check, authorizes settlement and bears execution or credit risk. A technology label does not replace that allocation.

Review requested: validate the proposed flow, liquidity commitment, settlement sequence, status evidence and commercial responsibilities before selecting a pilot corridor.

PARTNER REVIEW / 02 OF 07

One flow. One master reference.

The master reference is created before execution and remains immutable. Partner IDs, quote IDs, payout IDs, blockchain signatures and fee entries map back to it. A shared business reference coordinates multiple systems; it does not make bank, mobile money and blockchain actions a single atomic transaction.

Stage	Action and release condition
01 / Madiba Verify	Clear sender identity and required screening; validate recipient destination and account details. Apply the supported checks and review rules on pages 6-7. Phone validity alone does not prove ownership.
02 / Forex and quote	Record send amount, receive amount, currencies, FX rate, spread/fees, quote ID and expiry. Confirm that the rate is executable for the proposed route.
03 / Secure readiness	Obtain the liquidity provider's commitment ID, reserved amount, expiry and payout conditions. Confirm collection and payout availability. Do not collect on an expired or non-binding indication.
04 / Collect	Instruct collection once. Advance only on authoritative confirmation that meets the liquidity provider's acceptance criteria; a pending callback is insufficient.
05 / Convert and pay	Provider converts or hedges under the locked terms and uses committed local liquidity to execute payout. Record acceptance separately from final delivery confirmation.
06 / Settle and reconcile	Execute agreed USDT settlement on Solana; monitor confirmation/finality; match collection, FX, payout and settlement records. Track payout and settlement as separate state dimensions.
07 / Distribute fees	Allocate agreed fees, including Madiba's, and distribute when contractual release conditions are satisfied. Reconcile fee transfers, reversals and remaining balances.

Execution states and completion

Illustrative lifecycle: CREATED → VERIFIED → QUOTED → READY → COLLECTION_CONFIRMED → PAYOUT_PENDING → PAID. Settlement separately tracks NOT_STARTED → SUBMITTED → CONFIRMED → FINALIZED. Accounting closes as RECONCILED only after all required amounts and records match.

Key rule: collection proceeds only while an executable payout commitment remains valid. PAID requires payout-provider evidence; SETTLED requires the agreed blockchain finality evidence. Neither status substitutes for the other.

Every instruction uses an idempotency key. Signed callbacks are recorded with source, timestamp, sequence and raw evidence; duplicate or out-of-order events must not cause a second collection, payout or fee distribution.

PARTNER REVIEW / 03 OF 07

Liquidity first. Instant payout by design.

The conversion/payout logic pre-arranges local funds. After qualifying collection confirmation, the provider executes payout without waiting for incoming USDT settlement, if the agreed credit arrangement allows. This is the mechanism for instant local delivery; blockchain speed alone cannot supply local bank or mobile money liquidity.

1. Replacing Madiba's standing prefunding

Instead of Madiba maintaining a standing prefunded balance at the payout partner, the liquidity provider supplies its own funds or a committed credit facility and is reimbursed through the agreed settlement flow. Liquidity remains essential. The model relocates funding and timing risk to a contracted provider; it does not eliminate either risk.

If the provider requires finalized USDT before releasing local funds, payout must wait for that event. Partners must choose explicitly between credit-backed payout ahead of settlement and settlement-first payout; the system must not assume credit that has not been granted.

2. Minimum commitment terms to agree

Term	Required decision or evidence
Coverage and capacity	Countries, currencies, payout methods, operating hours, per-transfer and aggregate limits; committed local capacity and reservation expiry.
Binding trigger	Exact conditions that make the commitment enforceable; qualifying collection status; how reserved capacity is consumed and released.
Conversion execution	Locked FX rate or pricing formula; quote validity; slippage owner; when the provider converts or hedges and who covers asset-price movement.
Funding and credit	Who advances local funds; credit limit and tenor; settlement deadline; collateral, guarantee or reserve if negotiated; escalation on exhausted limits.
Payout promise	Measured time from qualifying collection confirmation to recipient credit; exclusions, delivery evidence, remedies and failed-transfer responsibility.
Settlement and default	Net/gross amount due; USDT network and finality policy; late settlement, collection reversals, provider default, insolvency and loss allocation.

3. Readiness gate and liquidity monitoring

Before collection, recheck quote validity, compliance clearance, partner health, available commitment capacity and payout-route availability. Record the decision against the master reference. Stop new collections if commitments cannot be honored; route to an approved alternative only with fresh readiness confirmation.

No unconditional speed promise: instant payout requires the provider's executable commitment and an available receiving rail. Define measurable service levels and recovery obligations; do not describe a reservation or payout acceptance as proof of recipient credit.

PARTNER REVIEW / 04 OF 07

Settlement, reconciliation and all fees

1. USDT on Solana: settlement evidence

Partners agree the supported USDT token/mint, Solana network, source and destination accounts, settlement amount, fee payer and authorization policy. Confirm wallet compatibility and maintain sufficient SOL for network costs. Validate addresses and token identity; never place private keys or personal recipient data in public transaction memos.

Solana distinguishes processed, confirmed and finalized states. The settlement contract must identify which state permits payout credit decisions and which closes the settlement obligation. Processed is not final; finalized is the strongest network confirmation state described in Solana's RPC documentation. [1]

Solana transaction instructions can execute atomically within a blockchain transaction. That atomicity does not extend to independent bank or mobile money delivery. On-chain fee distribution may be combined where technically supported, but a failed external payout still needs separate recovery logic. [2]

2. Reconciliation record per master reference

Record group	Minimum fields
Commercial and execution	Master reference; partner IDs; quote/commitment IDs; currencies; send and receive amounts; FX rate; pricing components; collection and payout statuses/timestamps.
Blockchain settlement	Network; token/mint; source/destination; token amount; signature; submission time; observed confirmation/finality; network costs and settlement acceptance.
Financial control	Expected vs actual balances; provider payable; each fee entitlement; distributions; refunds/reversals; residual amounts; exception owner and closure evidence.

3. Fee allocation and release

The fee schedule covers collection, FX/conversion, liquidity, payout, settlement/network costs and Madiba's agreed entitlement. Identify whether Madiba earns a spread share, explicit partner fee or both, so revenue is counted once. A zero customer-facing transfer fee does not imply that partner costs are zero.

Illustrative balance rule - all values in the agreed settlement unit:
Available settlement value = provider reimbursement + separately payable partner fees + Madiba entitlement + separately funded network cost + residual/refund balance.
Do not add fees already included in a net provider rate or reimbursement amount a second time.

Agree gross versus net settlement, rounding, fee currency, release timing, dispute windows and responsibility for failed-transfer costs. Mark RECONCILED only after payout, settlement and all required fee/accounting records match; an unmatched or pending fee leg remains open.

PARTNER REVIEW / 05 OF 07

Exceptions, pilot controls and partner sign-off

Exception	Required response
Quote / commitment expires	Do not initiate collection. Refresh pricing and capacity; obtain renewed customer acceptance if the payable amount or terms change.
Collection succeeds; payout fails	Confirm definitive failure, release unused capacity and start the agreed refund or approved reroute. Assign funding responsibility and track customer reimbursement.
Payout status is unknown	Query by original partner ID before retrying. Retain PAYOUT_PENDING or MANUAL_REVIEW; do not issue a second payout on a timeout alone.
Payout succeeds; settlement fails	Keep PAID intact, flag the provider payable as outstanding and recover under credit/default terms. Monitor exposure and suspend new collections if limits are exceeded.
USDT / network disruption	Pause affected settlement instructions; reconcile what actually landed. Any alternative rail requires supported wallets, approvals and agreed commercial treatment.

Pilot acceptance checklist

Commercial: execute the provider liquidity commitment, credit/settlement terms, fee schedule and service levels. Name responsible operating entities and approved corridor limits.
Technical: test successful flow, duplicate/out-of-order callbacks, quote expiry, insufficient capacity, uncertain payout, settlement delay, refund and fee reversal.
Evidence: demonstrate one master reference across every partner record, recipient-credit confirmation, blockchain finality and a balanced reconciliation report.
Operations: assign monitoring, on-call escalation, reconciliation ownership and customer support; prove pause/resume controls and recovery before launch.

Decisions requested from reviewing partners

1. Can you issue a binding conversion/payout commitment before collection, and for what capacity and duration?
2. Can you release local payout ahead of finalized settlement, and under which credit terms?
3. Do you support USDT on Solana, and what confirmation/finality closes your settlement obligation?
4. Which party owns refunds, failed-transfer costs, collection reversals and late settlement exposure?
5. Which APIs, status evidence and reconciliation files will you provide for a controlled pilot?

Proposed approval record: organization / named reviewer / role / approved corridor / capacity and limits / open conditions / target pilot date. Partner acceptance is documented separately; this paper itself creates no guarantee or execution commitment.

References and contact

[1] Solana RPC Overview - commitment states: solana.com/docs/rpc
[2] Solana Transactions - instruction-level atomicity: solana.com/docs/core/transactions
Technical references checked 25 October 2026. All other architecture, states and controls above are proposed Madiba design requirements.

Madiba Digitals Inc. - Delaware parent | Madiba Digitals Ltd - Nigeria operating subsidiary
Partner enquiries: info@madiba.digital | madiba.digital | SharpSharp.cash

MADIBA STANDARD / VERIFICATION LAYER

Madiba Verify

Sender identity verification + recipient verification, coordinated before collection.

Release gate: Sender clearance + recipient checks + valid quote + executable payout commitment. A completed SDK session alone does not satisfy this gate.

01 / Sender identity verification

Collect consent and link the verification session to the authenticated sender. Offer national ID or passport where supported; Nigeria may additionally offer BVN. Track database checks separately from document authenticity checks.

Coordinate live selfie, liveness and face comparison against an eligible reference image. Route failed, suspicious, missing or contradictory evidence to review. Apply sanctions screening and PEP review as distinct controls under the agreed rules.

02 / Recipient verification

Validate country, payout method, bank/account or mobile money details. Use account-name enquiry or authoritative partner confirmation where supported. Capture required beneficiary details and resolve material discrepancies before collection.

Record exactly what each provider checked. Phone formatting, validity and carrier detection do not establish the recipient's identity or account ownership. Unsupported checks remain marked unavailable; they are not treated as passed.

03 / One linked evidence record

Link sender clearance, recipient check reference, screening/review decisions, quote and liquidity commitment to the master transaction reference. Keep personal and biometric evidence in protected storage, never public blockchain memos.

Madiba owns the orchestration and decision workflow. Approved providers perform underlying checks. This architecture does not assert universal country coverage, automatic approval, partner acceptance or reseller rights.

MADIBA STANDARD / VERIFICATION LAYER

Clearance before collection

Proposed controls and acceptance tests for the Madiba Verify layer.

Separate status from approval

Suggested states: NOT_STARTED / IN_PROGRESS / RESULT_RECEIVED / REVIEW_REQUIRED / APPROVED / NOT_APPROVED / EXPIRED. Provider completion, document match and liveness scores are evidence inputs, not payment authorization.

Only a server-side decision against the approved country and partner policy can release the verification gate. Browser redirects, client claims, unsigned callbacks and unknown statuses must not grant clearance. Current live testing retains review-only results and keeps transfers paused.

Reuse evidence with defined limits

Bind approved sender evidence to the account, provider reference, country, verified method, policy version, decision time and expiry. Reuse only while valid under the agreed policy; changes in identity, risk, expiry or partner rules trigger refresh or review. Recheck recipient details when the destination changes.

Provider controls and review

Authenticate provider callbacks; deduplicate events; retain delivery evidence and the decision history. Treat timeouts and unavailable checks as unresolved. Route alternatives only when authorized and supported, without converting a failure into an automatic pass.

Use least-privilege access, retention/deletion rules and a lawful basis for personal and biometric processing. Confirm approved provider purposes, onward sharing, branding and contractual responsibilities before extending Madiba Verify to external clients.

Pilot acceptance evidence

• Successful sender and recipient checks; failed or suspicious document; missing live selfie; unsupported country/document type.

• Expired clearance, changed beneficiary, duplicate/out-of-order callback, invalid signature and unknown provider status.

• Review outcome and audit trail; evidence that collection remains blocked until every release condition is satisfied.

Partner sign-off must name who performs each check, who reviews exceptions, which evidence is accepted and who may authorize collection. The layer is a proposed implementation, not a claim of completed deployment.