KRG v0.1 WHITEPAPER

Offline State Synchronization Protocol (OSSP)

By BELLO MALAMI MUHAMMAD

2025

A protocol for trusted offline identity, payments, records, governance, and digital continuity using State Change Packets (SCPs).

ABSTRACT

Modern digital systems collapse the moment connectivity is lost , payments can not be made, identity verification fails, certificates cannot be validated, governance processes halt, and entire populations become digitally invisible.

KRG (Kinetic Relay Grid) introduces a new protocol class: the Offline State Synchronization Protocol (OSSP). It enables devices to exchange cryptographically verifiable state transitions offline through SCPs (State Change Packets), propagate them through multi-hop relays, preserve trust without servers, and finalize global truth through delayed reconciliation.

KRG is not a blockchain, not a mesh network, not DTN — it is a new foundation for offline digital trust.

1. INTRODUCTION

Every digital system today depends on connectivity.

When networks fail — in rural villages, urban outages, disasters, conflicts, or intentional shutdowns — digital trust breaks instantly.

KRG solves this by moving trust and state away from servers and into devices themselves, enabling digital systems to survive offline.

KRG provides:

- Offline identity verification

- Offline certificate issuance

- Offline payments and commerce

- Offline governance

- Offline aid distribution

- Offline medical and education records

- Trust propagation without infrastructure

2. WHAT IS KRG?

KRG is an Offline State Synchronization Protocol (OSSP).

It allows devices to:

1. Generate a state transition

2. Encode it as an SCP (State Change Packet)

3. Transfer it offline (Bluetooth, NFC, Wi-Fi Direct, QR)

4. Relay it through multiple offline hops

5. Store pending states

6. Finalize truth during reconciliation

KRG = offline truth + offline state + offline trust + delayed reconciliation.

3. WHAT ARE SCPs? (STATE CHANGE PACKETS)

Every State Change Packet (SCP) stores the following data

| prev_state_hash |

| new_state_hash |

| nonce |

| ttl |

| metadata |

| signatures (issuer + user) |

SCPs cannot be forged, reordered, modified, or replayed.

They are cryptographic truth that survives offline.

4. HOW OFFLINE STATE WORKS

Offline State Transition:

Previous State (S0) ----SCP----> New State (S1)

State normally lives on a server.

KRG moves state to the device.

Examples: identity updates, certificates, payments, attestations.

5. IDENTITY MODEL

Identity is represented as a sequential chain of SCPs:

- Identity_SCP

- Verification_SCP

- Attestation_SCP

- Certificate_SCP

- Revocation_SCP

Verification works offline through:

- signature checks

- hash integrity

- nonce order

- lineage continuity

- TTL validity

- revocation sets

6. CERTIFICATES & RECORDS

Authorities (WAEC, NECO, JAMB, schools, hospitals) issue certificates as SCPs.

A certificate SCP includes:

- issuer signature

- user signature

- metadata (grades, dates)

- lineage

- expiry

Anyone can verify certificates offline.

Forgery becomes impossible.

7. OFFLINE PAYMENTS

Payments are encoded as Payment_SCP.

Security mechanisms:

- nonce ordering (prevents double-spend)

- offline spending limits

- TTL (prevents replay)

- reconciliation (final settlement)

Merchants can safely accept payments offline.

8. MULTI-HOP PROPAGATION

Multi-Hop Relay (completely offline):

User A ---> User B ---> User C ---> (Eventually Online)

.

Relays cannot alter SCPs — they only transport them.

Store → Carry → Forward

9. SECURITY MODEL

KRG security includes:

- Ed25519 signatures

- Hash-chain lineage

- Nonce ordering

- TTL

- Canonical encoding

- Deterministic reconciliation rules

10. REVOCATION

Revocation is handled offline through:

1. Local revocation sets (from last sync)

2. Revocation SCPs propagating through relays

Offline devices still detect revoked IDs and certificates.

11. RECONCILIATION (GLOBAL TRUTH)

OFFLINE PHASE (SCP CREATION)

Device A -------->Device B --------> [Offline SCP Exchange] -------->Device C .....

- Identity SCPs
- Payment SCPs
- Certificate SCPs
- Revocation SCPs

(All collected offline, out of order)

ONLINE PHASE (RECONCILIATION)

| RECONCILIATION ENGINE |

Collect all pending SCPs

Validate signatures & hashes

Group SCPs by identity/account

Enforce nonce ordering

Detect & resolve conflicts

Apply valid state transitions

| Output: Final global state |

RESULT: ONE CONSISTENT, TRUSTED TRUTH

Reconciliation provides deterministic global truth and full auditability.

12. USE CASES

-Offline Identity Verification:

- Offline + certificate verification

- NIN/BVN offline identity

- police and law enforcement

- elections

- healthcare

- aid distribution

- offline payments

13. ARCHITECTURE OVERVIEW

1. Application Layer

   Identity, Payments, Records

2. SCP Layer

   State transitions

3. Relay Layer

   Store / Carry / Forward

4. Transport Layer

   Bluetooth, NFC, Wi-Fi Direct

5. Reconciliation Layer

   Final truth ordering

14. ROADMAP

v0.1 — Concept discovery

v0.5 — Reference implementation

v1.0 — Full specification

v2.0 — DKRG (Decentralized Grid)

v3.0 — DKRN (Decentralized Identity + Governance Network)

15.Conclusion

KRG introduces a new paradigm for digital trust: the ability for identity, payments, records, and governance to continue functioning even when the world goes offline.

By moving state and verification away from network infrastructure and into cryptographically verifiable packets exchanged between devices, KRG provides a foundation for resilience that has never existed in digital systems.

State can be created offline, verified offline, relayed offline, and only finalized when any device eventually reconnects. This makes KRG uniquely suited for the regions and scenarios where traditional connectivity is weak, costly, censored, or completely unavailable.

KRG is not a blockchain, not a mesh network, and not a traditional communication protocol. It is a new class of system — an Offline State Synchronization Protocol —designed to ensure that digital truth does not depend on Internet availability.

This v0.1 release defines the core primitives, conceptual model, and architecture. Future versions will refine the specification, formalize the SCP structure, introduce reference implementations, and expand KRG into DKRG (Decentralized Kinetic Relay Grid) and DKRN(Decentralized Kinetic Relay Network)for a large-scale decentralized identity and governance.

The world is increasingly digital, yet still fragile. With KRG, digital society gains a continuity layer that remains functional regardless of infrastructure. Connectivity becomes optional. Trust remains permanent.

KRG v0.1 marks the beginning of this journey.