

Flash Bingo 75

Multi.Bingo Live Bingo · Cert Pack v1

Engine: flashbingo-75

Region: BR

Cartela price: 50 cents · **Sale window:** 25s

Issued: 2026-05-15T23:01:22.327403Z · Authority: Multi.Bingo Bingo RGS

Signing key: Ed25519 · ID d651f1b9f793f40d

Game family

75-ball US-style Bingo · cartela 5x5 with FREE center · patterns: Linha / Linha Dupla / X / Coroa / Cartela Cheia

RTP target: 90.0% across 5 patterns

1. Round lifecycle

Rounds cycle every **25s** sale window + ball-draw phase. Flow: `sale_open` → `cartelas_minted` → `sale_close` → `ball_draw_seeded` → `balls_drawn` → `patterns_detected` → `settle` → `payout`. Cartelas are deterministically generated from `round_id` + `player_id` + `cartela_seq`; ball draws come from the RGS service `multibingo-rng:9443` per K.A.R. RNG requirements.

2. RNG service (mandatory)

All randomness comes from the certified RGS service `multibingo-rng:9443` (RNG_STRICT=true environment, no local `crypto.randomBytes` fallback). Each `round_id` is associated with a single `rng_draw_id`; balls drawn are `rngdraw(round_seed)[0..ball_count-1]` via Fisher-Yates over a 1..90 (or 1..75) integer array.

3. Audit chain (K.A.R. (h) compliance)

Each round persists: `round_seed_hash`, `ball_sequence_hash`, `cartela_root` (Merkle of all cartelas), and an Ed25519 signature (key ID `d651f1b9f793f40d`) over the round envelope. Daily Merkle root spans all rounds + tickets across all verticals (iLottery + Bingo + Keno).

4. Verifier endpoints

```
GET /api/bingo-ent/rooms
GET /api/bingo-ent/rooms/sala-4-flash/round/current
GET /api/bingo-ent/rounds/:round_id/audit
GET /api/ilottery/audit/public-key (shared signing key)
GET /api/ilottery/merkle/proof/:settlement_id (cross-vertical Merkle)
```

6. Operator Ed25519 public key

```
-----BEGIN PUBLIC KEY-----
MCowBQYDK2VwAyEAU2k0zXnm09QHduKLSEQYUAFeACAEOTUceEuiRGLSiXs=
-----END PUBLIC KEY-----
```