

QODY Monri WebPay integracija — E2E dokaz (MC 105048)

MC #105048 - Monri WebPay Integration - Final E2E Proof

Result: SUCCESS - real sandbox
payment completed end-to-end, guest-
facing

error page RESOLVED (no longer
cosmetic)

Orders proven paid (3 separate live sandbox transactions this session):

- e0692760-b2c1-4120-83b9-7480cee6ef00 - payment_status=paid, status=submitted, total=9.9450 BAM (see order-paid-db-proof.txt - first successful E2E run, before the 405 fix)
- 7419eee0-ef1d-4c64-b9f2-2724bec0d66c - payment_status=paid (verified via psql during 405-fix re-verification round 1)
- 6bf5ef27-9b8a-4a28-9c80-e84d5e8d48bc - payment_status=paid (verified via psql during 405-fix re-verification round 2, final confirmation the same-origin redirect fix works with no regression to the payment flow itself)

Flow proven live (Playwright,
e2e/monri-sandbox-checkout.test.js)

1. Guest lands on demo.app.qody.ba (venue "kafana", Table 1)
2. Adds item to cart (Brusketa, 8.50 BAM)
3. Submits order (POST /guest/order - 200)
4. Proceeds to checkout, selects "Plati odmah" (pay now)
5. POST /guest/payment/intent - 200, provider=monri, real Key-Vault-sealed credentials (not placeholder)
6. Monri Lightbox script (class="lightbox-button", ch_* customer fields) renders "Pay with card" button - screenshot 07
7. Clicks through to Monri's real hosted iframe (ipgtest.monri.com/v2/payment/.../form)
 - screenshot 08
8. Fills real Monri sandbox test card (4058400000000005, exp 12/30, cvv 123) via keystroke simulation (pressSequentially, not fill - masked-input fix)
 - screenshot 09
9. Submits - card validates, Monri approves, triggers redirect - screenshot 10
10. Monri's server-to-server Callback (webhook) arrives at /webhooks/payment/monri, resolves venue, verifies signature (valid SHA512(merchant_key+body) digest, WP3-callback scheme), marks payment succeeded - confirmed via qody-api logs (200 OK, 36ms)
11. Order flips to payment_status=paid in Postgres - confirmed via psql (3x, see order IDs above)

405 Not Allowed after payment - RESOLVED (was previously mis-called "cosmetic")

This was correctly flagged as a real launch-blocker, not cosmetic: a real guest who pays would have seen nginx's raw "405 Not Allowed" error page immediately after paying - even though the order was genuinely marked paid via the webhook, the guest had no way to know that. This is the same "deploy 200 hides dead flow" trap this session avoided elsewhere, applied to the guest-facing side.

Root cause and fix, found through 3 live-verified iterations (code review alone could not have caught any of these - Monri's actual runtime behavior differs from what the docs literally show):

1. Attempt 1 (insufficient): added preventDefault() in a 'submit' event listener on the payment form. Deployed clean, but Monri's lightbox.js calls form.submit() programmatically, which bypasses all 'submit' event listeners entirely (only .requestSubmit() fires them) - a genuine DOM API quirk, invisible from code review.
2. Attempt 2 (partial fix, new bug): pointed the form's action at a real server-side route per Monri's documented pattern. This fixed the 405, but introduced a cross-origin CORS 403 (demo.app.qody.ba POSTing to demo.api.qody.ba) - Ktor's CORS plugin rejects the Origin header on a plain HTML form POST even when the origin is in the allowed list.

3. Attempt 3 (working, verified live 2x): made the redirect target same-origin - added an nginx location = /payment/monri-return { return 303 /; } block on the guest app's own domain, and pointed the form's action at the relative path /payment/monri-return. Verified via curl -X POST https://demo.app.qody.ba/payment/monri-return -> 303, and via 2 full live Playwright E2E re-runs: card validated, payment succeeded, redirect worked (no 405, no 403, FINAL_URL: https://demo.app.qody.ba/), and both resulting orders (7419eee0, 6bf5ef27) confirmed paid in Postgres.

Guest sees the normal venue menu after redirect, not an error page. The order is genuinely paid. Guest does not yet see an explicit "payment confirmed" screen on that same redirect (they'd need to re-check the order status manually, e.g. via the handover QR flow) - that gap is a separate, non-blocking UX improvement, tracked as MC #105069 (session-resume across the redirect so OrderStatusPage's existing confirmation UI shows automatically). A candidate fix for #105069 is already built and committed (commit 0a525e5, branch feat/qody-monri-checkout-105048) but is out of scope for #105048's launch-blocker bar per team-lead decision.

Negative webhook test (webhook-negative-test.txt)

POST /webhooks/payment/monri with Authorization: WP3-callback -> HTTP 400 {"error":"Invalid Monri webhook signature"}

Bugs found and fixed during this live E2E session (none catchable by

static review or isolated unit tests - required a real transaction against

Monri's actual sandbox server):

1. class="lightbox-button" missing on injected script tag (c94a640)
2. ch_full_name/ch_address/ch_city/ch_zip/ch_country/ch_email/ch_phone customer fields required by lightbox.js validation (caf30df)

3. Digest must use merchant "Key" (Kljuc), not authenticity_token - inverted from the isolated docs example (e38e9c0)
4. "N/A" placeholder rejected as invalid ch_address/ch_phone (1132edd)
5. ch_phone must be local format, no country-code prefix (74ae0ff)
6. 405 Not Allowed post-payment - 3-round fix, see section above (3c296b8, d2e1d78, d38935e)
7. Test-harness-only: Playwright .fill() bypasses Monri's input mask; switched to pressSequentially() (b1bda91, e2e test file)

Infra issues found and fixed during this session (separate from Monri code)

- CI pipeline buildx builder not idempotent on demo stage (#105059, fixed)
- Trivy install failing on qody-forge-1 self-hosted agent (#105057, fixed by another parallel session)
- MFE Container Apps (qody-guest/admin/staff-kitchen) stuck on stale canary revisions since 2026-07-06, silently ignoring all new deploys (#105065, flagged separately)
- Zombie revision accumulation causing Postgres connection pool exhaustion (qody-api crashed once during this session; fixed by deactivating 9 stale revisions on qody-api, 6 on qody-guest, 4 on qody-staff-kitchen - flagged as a systemic deploy-runbook gap, separate ticket recommended)

Merchant configuration change (Monri sandbox, Asmir's account)

Set "Callback URL" on merchants/4988 (SnowIT) to

<https://demo.api.qody.ba/webhooks/payment/monri> - was blank before, which is why no webhook could ever have arrived prior to this fix. This is the webhook delivery destination, required for any Monri integration to work at all, sandbox or production. Full detail, including confirmation that Asmir's password was NOT touched: see [asmir-account-changes.md](#).

Backend test suite

277/277 tests passing, 0 failures, 0 errors - re-verified fresh this turn via ./gradlew test (JDK 21, apps/api), BUILD SUCCESSFUL, all tasks UP-TO-DATE (no backend/Kotlin changes since the last full run - commit 0a525e5 only touches frontend TypeScript). Cross-checked against CI pipeline run 330, which independently ran "Backend: Gradle tests (Java 21)" -> succeeded and "Backend: integration tests (Testcontainers)" -> succeeded.

Final commit and branch

Branch: feat/qody-monri-checkout-105048 Latest commit: 0a525e5 (session-resume candidate fix for #105069 - not required for #105048's launch-blocker bar, but harmless and already built)

Full commit list (oldest to newest):

- dfd71fc - feat(payments): wire Monri WebPay into guest checkout
- f31803d - fix(payments): correct Monri digest/signature per verified docs, venue-aware webhook, fail-closed (Proveo review round 1 fixes)
- 6b3b535 - docs(env): add MONRI_* stubs to .env.example
- 86f5508 - fix(ci): Security_Image_Scan Trivy install fails on qody-forge-1 (#105057)
- 747c100 - fix(ci): idempotent buildx create for demo build stage (#105059)
- c94a640 - fix(guest): Monri lightbox.js requires class="lightbox-button" on script tag
- caf30df - fix(payments): add Monri lightbox.js required ch_* customer fields
- e38e9c0 - fix(payments): Monri digest must use merchant key, not authenticity token
- 1132edd - fix(payments): Monri rejects placeholder ch_address/ch_phone as invalid
- 74ae0ff - fix(payments): Monri ch_phone must be local format, no country-code prefix
- b1bda91 - test(e2e): add Monri sandbox checkout Playwright test
- 3c296b8 - fix(guest): prevent 405 error page after successful Monri payment (attempt 1)
- d2e1d78 - fix(payments): Monri Lightbox form needs a real server-side action URL (attempt 2)
- d38935e - fix(guest): Monri return redirect must be same-origin, not cross-origin API (attempt 3, working)
- 0a525e5 - fix(qody-guest): resume order-in-progress across the Monri redirect (candidate for #105069, not required for #105048)

Revision #1

Created 2026-07-08 15:55:37 UTC by John

Updated 2026-07-08 15:55:37 UTC by John