CHECKOUT 2.0 / MERCHANT BACKEND

Technical Manual - Checkout 2.0

KONEBE Smart Checkout - store sends the amount and buyer selects the asset

1. What Checkout 2.0 is

Smart Checkout lets the store send the price, commercial currency and order reference. The buyer selects the cryptocurrency within KONEBE Checkout. The merchant needs its own backend.

> The initial session must not create blockchain charges for every asset. The definitive charge is created only after the buyer confirms the selected asset.

2. Create an authenticated session

```
POST /api/merchant-checkout
Authorization: Bearer <PDV_KEY_SERVER_ONLY>
Content-Type: application/json

{
 "action":"session-create",
 "externalId":"ORDER-1001",
 "currency":"BRL", "amount":"150.00"
}
```

The backend validates the connection, enabled assets, settlement mode and limits. The response may contain ok, reused, session and paymentUrl. Keep the commercial reference and redirect using the returned URL.

3. Buyer selects the asset

• The checkout displays the merchant name, commercial amount and only the authorized cryptocurrencies.

• The KONEBE page uses session-get and session-choose without exposing the PDV Key in the browser.

• After selection, it displays the network, final amount, authorized address, QR or link, deadline and status. Never present an estimate as the definitive quote.

4. Check the order on the server

```
POST /api/merchant-checkout
Authorization: Bearer <PDV_KEY_SERVER_ONLY>
Content-Type: application/json

{"action":"session-status","externalId":"ORDER-1001"}
```

Only session.status=paid authorizes automatic fulfillment. Retrying with the same reference after a timeout prevents duplicate charges. Conflicting parameters may trigger 409.

5. Expiration, errors and safeguards

• Expired session: start a new session only through an authorized business flow; never mark the old one as paid.

• Quote error: show an unavailable state, not fictional prices. Disabled asset: do not offer or accept that asset.

• Never place the PDV Key in frontend code, URLs or QR codes. Monitor results through authenticated requests from the store backend.

Security and financial limits

• Never share recovery phrases, private keys, the PDV Key or treasury credentials with buyers; never embed them in public HTML.

• Only backend-confirmed status=paid authorizes automatic order fulfillment. Opening a link, scanning a QR code or receiving HTTP 200 is not proof of payment.

• Converted settlement: at least 1 PEURO equivalent and a configurable maximum of up to 10,000 PEURO per charge; fees are set by the backend.

• Direct receipt: pre-authorized wallets, unique deposit addresses per charge and network-specific technical restrictions; the PEURO reserve limit does not apply.

Verification directly in production

KONEBE verifies operations directly in production after an authorized release, with monitoring and controlled amounts. This document does not certify deployment or real payments.

• Before testing, verify the actual API origin, checkout, Cloudflare bindings and D1 schema. Do not apply migrations automatically based on this manual.

• Use traceable order references, monitor blockchain reconciliation and record results without secrets.