CHECKOUT 3.0 / STATIC HTML

Technical Manual - Checkout 3.0

KONEBE Easy Checkout for Websites - HTML widget with KONEBE backend

1. What Checkout 3.0 is

Easy Checkout for Websites provides a payment widget for static HTML pages. Merchants do not need to build their own backend, but must activate an authorized KONEBE commercial connection.

> The public HTML contains only a widget identifier. Never include the PDV Key, recovery phrases or administrative privileges in external HTML.

2. Configure and enable the widget

• In Peuro Pay > Connections, open Easy Checkout for Websites 3.0. If needed, configure the POS, save preferences and activate the commercial connection.

• Choose a name, description, donation (variable amount) or payment (fixed amount), commercial currency, enabled assets and authorized HTTPS domains.

• Save and copy the generated HTML. Disabling a widget prevents new payments but does not cancel payments already in progress.

3. Embed in static HTML

```
<div class="konebe-checkout"
 data-widget-id="<PUBLIC_WIDGET_ID>"></div>
<script async
 src="https://app.konebe.com/app/checkout-widget-embed.js">
</script>
```

The script loads a KONEBE-hosted iframe. Use the actual public ID generated in the dashboard. Check behavior on sites enforcing Content Security Policy (CSP) and HTTPS origin restrictions.

4. Checkout API operations

Operation	Permission
widget-list / widget-save	Authenticated wallet session; saving requires an active connection.
widget-disable	Can disable even if the connection is inactive.
widget-get	Public read restricted to display information.
widget-start	Starts a public payment attempt with limits and identifiers.

All use POST /api/merchant-checkout. The backend controls recipients, assets, limits and permissions. Visitors cannot replace the recipient wallet.

5. Donations and fixed amounts

• Fixed amount: the backend uses the merchant-configured price; visitors cannot override it in HTML.

• Donation: the visitor enters an amount subject to authorized rules and converted-settlement limits when applicable.

• Each payment attempt has its own identifier. Retries of the same attempt must be idempotent; separate donations receive distinct identifiers.

6. Security and public-use limits

• Allowed domains are an additional safeguard: Origin and Referer headers do not authenticate on their own. Check CSP, iframe rules, request limits and revocation.

• The frontend cannot decide the recipient wallet, fees, conversion or payment confirmation. The backend verifies the network, transaction and payment status.

7. When to choose Checkout 2.0 instead

For orders with inventory and automated fulfillment integrated with the merchant backend, use Checkout 2.0 or the POS API. Checkout 3.0 is designed for simple payments on backend-free websites.

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.