POUŽITIE CDPAY API

s presmerovacou stránkou

Tento dokument popisuje použitie CryptoDiggers CDPAY API s presmerovacou stránkou (bez použitia iframe) pre vlastné implementácie podporovaných digitálnych mien do Vašich webových portálov.

Prostredia CDPAY:
Test: https://www.cryptodiggerstest.eu/api
Live: https://www.cdpay.eu

Redirect endpoint: redirect.php

Platba pomocou presmerovacej stránky sa vykonáva v 3 krokoch:
1. Vygenerujte presmerovaciu linku, aby sa zobrazila platbná brána
2. Vytvorte návratovú stránku pre stavy success/failure/timeout platby
3. Vytvorte callback stránku pre stavy success/failure/timeout platby

!!! HTTP metóda volania presmerovanej stránky musí byť typu GET. Všetky parametre sú povinné:

timeout	-	integer hodnota, 5 - 30
order_id	-	reťazec , dĺžka 1-50, povolené alfanumberické znaky 0-9, +, '-', '_'
amount	-	decimal hodnota , 0.10 - 20000
currency	-	integer hodnota:

- EUR=1
- USD=2
- CZK=16
- GBP=3
- CAD=4

- AUD=5
- JPY=9
- CNY=13
- AED=17
- PLN=18
- CHF=23

currency_crypto - integer hodnota:

- BTC=6
- LTC=8
- DASH=19
- XMR=20
- ZEC=21
- BCASH=24

Nonce - vždy sa zvyšuje o beznamienkových 64 bitov integer
timestamp - aktuálny Unix timestamp
order_id - string hodnota, dĺžka 1-50,
povolené alfanumerické znaky 0-9, +, '-',
'_'
returnAddress - Používateľsky definovaná redirect stránka pre versiu V2, musia byť URL encodované

api-key - CDPAY používateľský API kľúč
api-sign - Podpis správy je s base64 encodingom použitím HMAC-SHA512 a pozostáva z:*Test/Live CDPAY URL +'?' + < all get parameters except api-signature >*

Príklad pre redirect verziu 1 (krypto mena definovaná vopred):

https://www.cdpay.eu/redirect.php?order_id=asidf111as&amount=10.1&currency=1&currency_crypto=6&wait=0&timeout=6&api-key=c70ea0e0-1454-11e6-8eeb-00155d00c800&timestamp=1534498676&nonce=1534498676199779&api-sign=ejZ38gAtuZh2AK%2Bdch1GQhBfFiBuXEKToeB5%2FJHOzGLUxojrHyNcRDsSSEmMfhb6OOyN4UJRiDqQYFAMExFcNg%3D%3D

Príklad pre redirect verziu 2 (krypto mena definovaná užívateľom):

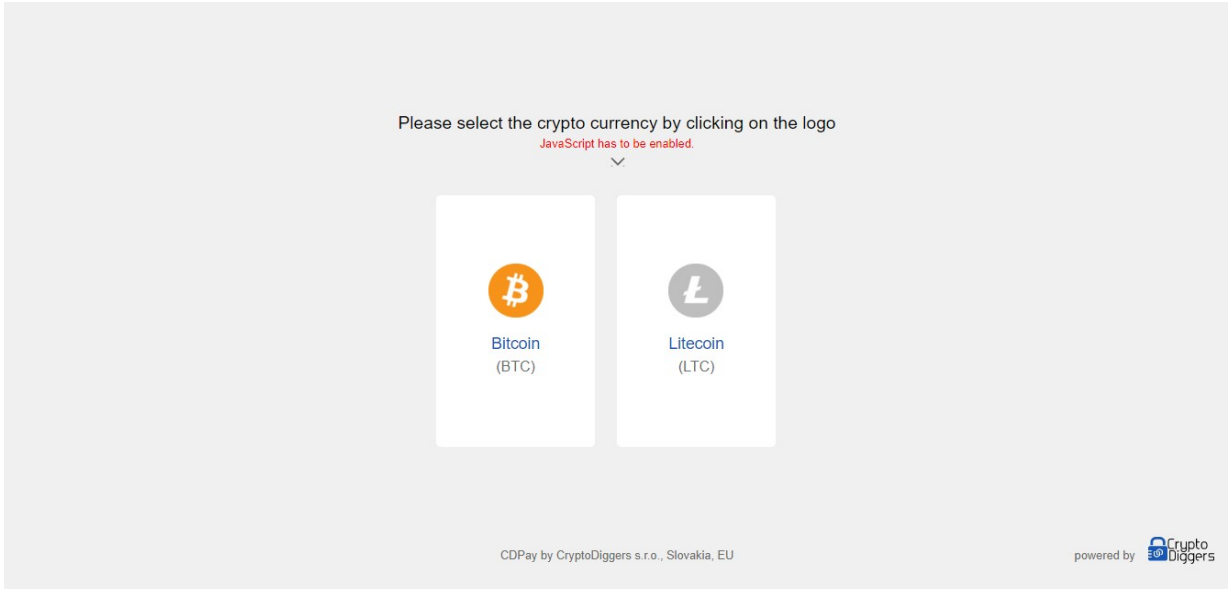
https://www.cdpay.eu/redirect2.php?order_id=1223&amount=5&currency=1&wait=0&timeout=15&api-key=bc5228b4-865e-11eb-8cfc-00155dfb8403&timestamp=1641650126&nonce=1641650126511172&api-sign=wS9u5T%2B16tdQ%2F2FC%2BO1efvZ%2FtQ633u5SFCOQLCkHPC3gIRoblVk29vKtQvPsjVjCu90rHwA%2Fq%2Bly4hOoATcsCw%3D%3D

Example for redirect version 2 (krypto mena definovaná užívateľom spolu s redirect stránkou):

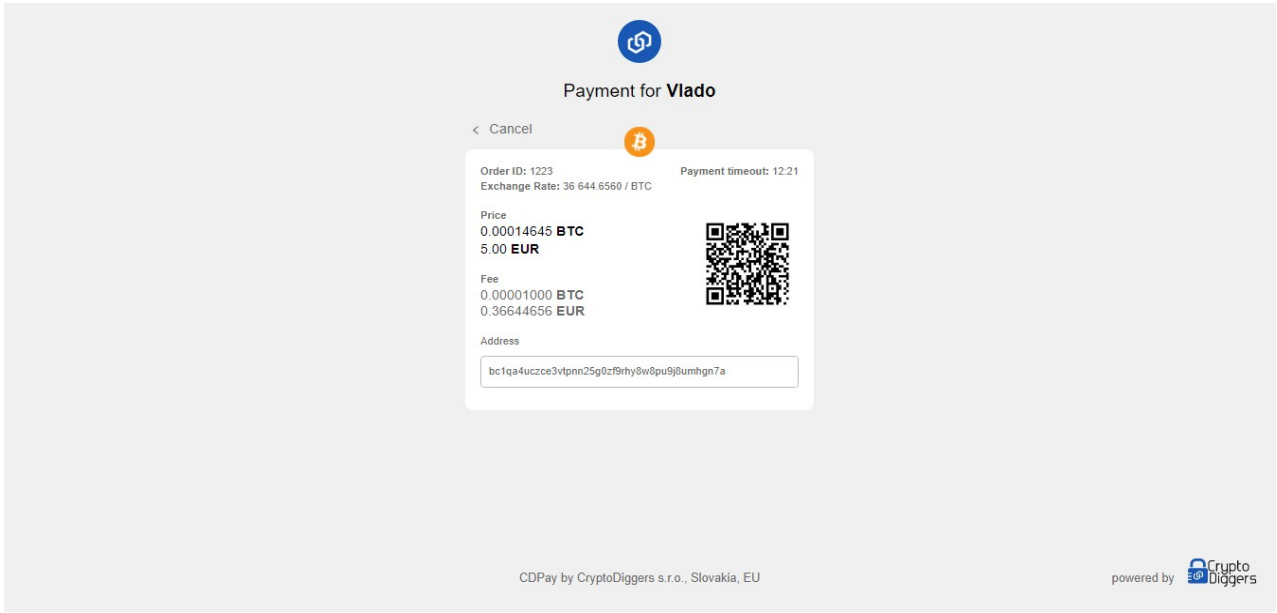
https://www.cdpay.eu/redirect2.php?order_id=1223&amount=5&currency=1&wait=0&timeout=15&returnAddress=https://www.your_redirect_page.com&api-key=bc5228b4-865e-11eb-8cfc-00155dfb8403&timestamp=1641650126&nonce=1641650126511172&api-sign=wS9u5T%2B16tdQ%2F2FC%2BO1efvZ%2FtQ633u5SFCOQLCkHPC3gIRoblVk29vKtQvPsjVjCu90rHwA%2Fq%2Bly4hOoATcsCw%3D%3D

Príklad ako vytvoriť API-Sign parameter v PHP:

```
const CDPAY_TEST_WEB="https://www.cryptodiggerstest.eu/api/redirect.php";
$apikey='Vaše API key';
$seckey='Váš SecKey';
$inputs["order_id"]='OrderTest-06';
$inputs["amount"]=10.10;
$inputs["currency"]=1;
$inputs["currency_crypto"]=6;
$inputs["wait"]=0;
$inputs["timeout"]=5;
$inputs["api-key"]=$apikey;
$inputs["timestamp"] = time();
$nonce = explode(' ', microtime());
$inputs['nonce'] = $nonce[1] . str_pad(substr($nonce[0], 2, 6), 6, '0');
$sign = base64_encode(hash_hmac('sha512', CDPAY_TEST_WEB .'?'. http_build_query($inputs, '', '&'), $seckey, true));
$inputs["api-sign"]=$sign;
echo "<a href='".htmlentities(CDPAY_TEST_WEB .'?'. http_build_query($inputs, '', '&'))."'
target='_blank'>".htmlentities(CDPAY_TEST_WEB .'?'. http_build_query($inputs, '', '&'))."</a>";
```



Prosím vyberte z podporovaných a s Vami v profile uloženými kryptomenami



Prosím pošlite zobrazené množstvo kryptomeny na procesovanie platby.

2. Na obrázku vyššie je zozbrazená presmerovacia stránka (v redirect verzii V2 môže byť definovaná vo volaní API parametrom returnAddress) CDPAY počas času trvania platby. Návratová URL linka je volaná v prípade nasledujúcich stavov platby *successful* / *unsuccessful* alebo *payment was not received*. Spracovanie návratovej stránky používa HTTP metódu GET.

Get parametre:

nonce	-	vždy sa zvyšuje o beznamienkových 64 bitov integer
timestamp	-	aktuálny Unix timestamp
status	-	status platby **0** – platba nebola prijatá **1** – platba bola prijatá, ale nie je potvrdená **3** – platba bola prijatá, ale v nesprávnej veľkosti
api-key	-	CDPAY používateľský API kľúč
api-sign	-	Podpis správy je s base64 encodingom použitím HMAC-SHA512 a pozostáva z: *CallBack URL +'?' + <all get parameters except api-sign parameter>*

Príklad:

```
https://www.eshopcallback.com/index.php?a=dsfdsf&timestamp=1534505380&nonce=1534505380020122&order_id=asidf111as&status=1&sign=BPDc43g2LjweLZ6gfkHBOU82EEQhh%2F9q%2BH4zGpoovU9PSgNqNePu3m0r3Wsi2ypeH45I0EoCEgMBtDvoEyRn%2FA%3D%3D
```

Príklad ako vytvoriť API-Sign na validáciu návratovej hodnoty:

```
$request["timestamp"] = time();
$nonce = explode(' ', microtime());
$request['nonce'] = $nonce[1] . str_pad(substr($nonce[0], 2, 6), 6, '0');
$request['order_id']='Your order ID';
$request['status']='payment status id';
$sign = base64_encode(hash_hmac('sha512', $user_callback_url. (strpos($user_callback_url,
'?')===false?'?':'&') .http_build_query($request, '', '&'),$SecKey, true));
$request['sign']=$sign;
$url=$user_callback_url.(strpos($_SESSION["user_callback"],'?')===false?'?':'&').http_build_query($request, '', '&');
```

3. CALLBACK

Parametre HTTP hlavičke:

API-Key	-	CDPAY používateľský API kľúč
API-Sign	-	Podpis správy používa HMAC-SHA512 a pozostáva z: *URI callback path +'? + SHA256(nonce + timestamp + POST data)*

Content type požiadavky musí byť nastavený na: **Content-type: application/json**

nonce	-	vždy sa zvyšuje o beznamienkových 64 bitov integer
timestamp	-	aktuálny Unix timestamp
POST data	-	sú posielané vo formáte JSON objektu

Majte na vedomí, že nonce nejde v žiadnom prípade vynulovať alebo znížiť na nižšiu hodnotu v čase. Jediný spôsob ako vynulovať nonce je vygenerovaním nového tajného kľúča v CDPAY portály, čo zníži hodnotu nonce na 0.
Čas na Vašom serveri musí byť synchronizovaný , aby ste mohli pracovať korektne s CDPAY API.

Všetky odpovede budú obsahovať dve JSON premenné:

- **error** – integer hodnota 0 alebo 1. 0=bez chyby, 1=chyba
- **error_msg** – reťazec hodnota – popis chyby

Funkcionalita Callbacku je používaná na aktualizáciu statusu platby. Štandardné spracovenie platby prebieha s nasledujúcimi statusmi:
0 – payment not received (platba nebola prijatá) – tento status je predolený a nezasiela sa
1 – payment received but not confirmed (platba prijatá, ale nepotvrdená)
2 - payment received and confirmed (platba prijatá a potvrdená)
3 – payment received but with incorrect amount (platba prijatá v zlej veľkosti)

Callback je vykonávaný z CDPAY API servera každých 15 sekúnd kvôli aktualizácii stavu platby. HTTP hlavička obsahuje podpis na verifikáciu, či dáta neboli pri prenose zmenené.

Proces verifikácie je ten istý ako pri ostatných API volaniach.

API-Sign = Podpis správy používa HMAC-SHA512 a pozostáva z:

CallBack URI cesta + SHA256(nonce + timestamp + POST data) a secret kľúč

Príklad v PHP:

```
$sign = base64_encode(hash_hmac('sha512', $eshop_url_callback.hash('sha256', $nonce . $timestamp . http_build_query($data, '', '&'), true), $secret, true));
```

Dáta odoslané callbacku vyžadujú nasledovnú implementáciu na strane eshopu:

Content type pre callbackovú funkciu: **“application/json”**.

txid – reťazec hodnota, obsahuje transakčné ID danej virtuálnej meny

order_id – reťazec hodnota, dĺžka 1-50,
povolené alfanumerické znaky 0-9, +, ‘-’, ‘_’

amount – decimalna hodnota, 0.10 - 20000

currency – integer hodnota:

- EUR=1
- USD=2
- CZK=16
- GBP=3 🕐 CAD=4
- AUD=5
- JPY=9
- CNY=13 🕐 AED=17
- PLN=18
- CHF=23

currency_crypto – integer hodnota:

- BTC=6
- LTC=8
- DASH=19
- XMR=20
- ZEC=21
- BCASH=24

status – integer hodnota, 0 - 3

timestamp – aktuálna časová pečiatka (timestamp) z CDPay API

nonce – integer hodnota, vždy vyššia hodnota ako predchádzajúca

JSON príklad:

{"txid":"0aa65e9cac6425f640c6c4b76398325d2c6cc44f6b66d8bf752a46de914eac43","amount":10,"order_id":"Order 1","status":1,"currency":1,"currency_crypto":8}

Stránka Callbacku musí odpovedať HTTP kód 200, výlučne s hodnotami true / false.