CDPAY volania platobnej brány

CryptoDiggers s.r.o.

Autor: CryptoDiggers s.r.o.

Verzia: v1.2

Dátum editácie: 13.06.2018

CDPAY volania pre vytvorenie platby

Platobná brána **môže/nemusí** byť implementovaná ako iframe do akejkoľvek HTML stránky.
Na to, aby ste ho mohli použiť bude nutné zavolať 2 volania REST API rozhrania a 1 kontrolné:

1. Na vytvorenie a obdržanie iframe id musíte volať linku na pozadí podľa inštrukciií v **KROK 1**. Toto volanie musí byť vykonané s Vašim API key a ďalšími parametrami. Nesmie byť viditeľné na stránke. Návratové hodnoty su nizžšie uvedené ako Response a je možné pomocou nich zostaviť vlastné rozhranie s QR kódom a platobnými údajmi za dodržania *timeout* hodnoty pre daná platbu. Adresy pre jednotlivé meny sa neopakujú, pre každú platbu je generovaná jedinečná adresa pre danú digitálnu menu.

2. Druhé volanie je volaním na zobrazenie iframe-u na Vašej stránke **KROK 2**. Pri zavolaní iframe id viac krát sa Vám môžu vyskytnúť nasledovné stavy:

   a. Ak nevypršal čas definovaný v hodnote „timeout“, zobrazí sa Vám ten istý iframe a čas pokračuje kontinuálne ďalej až pokiaľ nevyprší alebo používateľ nezaplatí
   b. Ak čas vypršal, odpočítavanie začne od znovu a prepočíta sa hodnota digitálnej meny voči aktuálnemu kurzu.
   c. V prípade, že platba správnej sumy bola poslaná v danom časovom limite, zobrazí sa Vám oznam „*Payment processed, please finish your order*.“ Tu je možné zobraziť finálne tlačidlo na stránke na ukončenie objednávky/platby.
   d. V prípade, že platba poslaná v nesprávnej hodnote v danom časovom limite, zobrazí sa Vám oznam „*You have sent incorrect amount of virtual coins to the generated address. Please contact eshop for more information*“ . V tomto prípade je nutný manuálny zásah a kontaktovať CryptoDiggers Helpdesk na email helpdesk@cryptodiggers.eu , helpdesk web https://cryptodiggers.freshdesk.com alebo volať na hotline číslo +421-907-826-087.

3. Tretím kontrolným volaním je volanie z **KROK 3**, ktoré preverí stav platby a vráti ich stavy popisané v **KROK 3**. Tieto stavy je vhodné preveriť kedykoľvek po procese zobrazenia iframe resp.platobných údajov.

Implementácia callback funkcionality a ako to funguje (krok za krokom):

1. **Ako nastaviť callback**
   a) Na to, aby ste mohli využiť funkcionalitu callbacku budete si ju musieť buď naprogramovať sami, pokiaľ používate vlastný typ eshopu alebo iný ako je v zozname (Magento 1.9, OpenCart 2.0, 2.2, Woocommerce). Callback je funkcionalita, ktorá počúva na parametre volané podľa špecifikácie parametrov nižšie na vašom portály. Zabezpečuje volanie, ktoré aktualizuje váše číslo objednávky do stavu "zaplatené alebo zprocesované" po obdržaní požadovaného množstva konfirmácií na použitej digitálnej mene pre platbu. Je preto dôležité implementovať ho správne a zabezpečene.

   Pretože ináč môžete čeliť útoku dvojitého zaplatenia (double spend) ak nastavíte objednávku priamo do stavu Zaplatená alebo Zprocesovaná.

   Statusy objednávok musia mať nasledovné poradie: najskôr „Akceptovaná / Održaná" a po dosiahnutí požadovaného počtu konfirmácií na použitej digitálnej mene, zavolaná callback functionalitou a aktualizovaná na vašom portály na "Zaplatená/Zprocesovaná" naprogramovanou funkcionalitou callbacku (v našom plugine, alebo vami doprogramovanym vlastným programom).

   b) Na zfunkčnenie callbacku budete potrebovať nastaviť URL vašej stránky (v prípade používania vlastného e-commerce portálu môžete vložiť celú linku a nastavit typ na *„custom"*) in the CDPAY portal in your profile in the section "User -> Add Callback".

   c) Callback požaduje nastavenie tak zvaného "Callback Secret" čo je vlastne heslo, ktorým spravíte mixing (osolenie) hashu z transakčného ID pri platbe "digitálnou menou" (BTC, LTC, DASH, etc.) a vaším heslom. Táto hashovania funkcia používa štandardný SHA512, ktorý je následne vložený a posielaný v parametri *„cdp_hash"* callbackom na vašu stránku. To vyžaduje dodatočnú akciu rovnakáho hashovania na vašej strane použitím SHA512 spojením = heslo (toto musí byť bezpečne uložené na vašej strane a zhodné s heslom pre callback vo vašom profile na CDPAY) + *„txn_id"* (poslané callbackom ako parameter) . Následne tieto dva hashe musia byť porovnané a platba zmenené, akceptovaná len v prípade ich zhody, ináč sa vystavujete

riziku, kde útočník môže zmeniť parametre pomocou útoku zvaného *man-in-the-middle*. Pre URL callbacku VŽDY použite HTTPS (certifikát) na vašej strane.

d) V prípade, že ste náš merchant (v našej správe) požadujeme len dodanie URL adresy, ktorá ma byť volaná callback funcionalitou z CDPAY portálu.

e) V prípade, že si spravujete svoj profil CDPAY, musíte si nastavenie callbacku spraviť pre každú menu, ktorú akceptujete na CDPAY portaly separátne.

f) Úkažka vo videu na YOUTUBE [01:40]

2. **Callback parametre**
Callback vracia návratové parametre a ich hodnoty v POST atribútoch.

Atribúty sú následovné:

a. **cdp_hash** -> tento atribút obsahuje Váš security kľúč a TransactionID peňaženky pre callback hašované s sha512 = “heslo ku callbacku” + “txn_id” poslane callbackom ako parameter, hashované s SHA512.

b. **txn_id** -> obsahuje TransactionID peňaženky.
Odporúčame porovnať hodnotu sha512 Vášho kľúča a tejto hodnoty s the cdp_hash hodnotou.

c. **amount** - > reálna hodnota digitálnej meny

d. **status** -> stav spracovania
   i. **1 – platba prijatá ale nepotvrdená**
   ii. **2 – platba prijatá a potvrdená**
   iii. **3 – platba prijatá so zlou hodnotou**

e. **order_id** -> Váše interné číslo objednávky, variabilný symbol danej platby.

KROK 1

ZOBRAZENIE ÚDAJOV NA NOVÚ PLATBU

Request:
https://www.cdpay.eu/api.php?apikey=YOUR_API_KEY&a=new_address&timeout=15&order_id=Order6661&amount=5.00&currency=1&currency_crypto=8&wait=0

Response:
{"address":{"address_value_out":"LS2RuWYejhSUGBE45kWRheLhpnYGBg7SRq","amount_out":"0.03262017","iframe_id":"ede0ee2a-9b2b-11e4-b228-00155d006403","currency_id_out":8,"currency_out":"ltc","Msg":"OK"},"error":0,"error_msg":""}

- **timeout** – povolené hodnoty od 10 do 30, integer, celé čísla (minúty)
- **order_id** – VS (variabilný symbol, jedinečný identifikátor klientskej platby) – môže obsahovať len číselné hodnoty (0-9), písmená (a-Z) nie je senzitívne na veľkosť, znaky (_ , -), dĺžka do 20 znakov
- **amount** – hodnota FIAT peňazí (FIAT=EUR,USD,..), desatinný oddelovač musí byť "." (bodka)
- **currency** – typ FIAT meny podľa číselníka, hodnoty (1,2,3,4,5,9,13,16,17) – EUR=1, USD=2, GBP=3, CAD= 4, AUD=5, JPY=9, CNY=13, CZK=16, AED=17, 18=PLZ, 22=VND, 23=CHF
- **currency_crypto** – hodnota digitálnej meny (6,8,19,21,24) – 6=Bitcoin(BTC), 8=Litecoin(LTC), 19=DASH, 21=ZCASH, 24=BCASH
- **wait** – čakanie na konfirmácie – povolené hodnoty (0,1) – **0=No**, 1=Yes (odporúčam nastaviť na 1)

KROK 2

ZOBRAZENIE QR KÓDU PRE PLATBU

Request:
https://www.cdpay.eu/api.php?iframe=17a2307c-0fd2-11e6-b5de-00155d000116&a=eshop_payment_v2&amount=5.00

Response:

iframe – UUID jedinečný reťazec, generované funkciou

apikey - Váš APIKEY

a - eshop_payment_v2 – typ volania, statická hodnota

amount – hodnota FIAT peňazí (FIAT = EUR,USD, ..) , desatinný oddelovač musí byť "." (bodka)

QR kód s platobnými informáciami sa dá zobraziť aj samostatne a to podľa nasledovných inštrukcií :

QR kód pre API:

http://www.qrcode.com/en/about/standards.html

Reťazec, ktorý je ukrytý za QR kódom ako URI:

<virtual_currency_name>:<wallet_address>?amount=<amount_virtual_currency>?label=<label>?message=<message>

Dáta v URI:

virtual_currency_name = <*bitcoin*|*litecoin*|*worldcoin*> - musí byť malými písmenami

wallet_address = adresa peňaženky vygenerovaná metódou **KROK 1** *New_Address* v odpovedi

API amount = decimal value of virtual currency, decimal separator is "."

label = string data - URI encoded

message = string data - URI encoded

KROK 3

KONTROLA STAVU PLATBY PODĽA IFRAME ID

Request:

http://www.cdpay.eu/api.php?iframe=17a2307c-0fd2-11e6-b5de-00155d000116&a=get_iframe_status

Response:

V prípade, že bola platba prijatá:
{"error":0,"error_msg":"","status_msg":"Payment processed, please finish your order.","status_id":1}

Zákazník poslal nesprávnu hodnotu digitálnej meny na adresu:
{"error":0,"error_msg":"","status_msg":" You have sent incorrect amount of virtual coins to the generated address. Please contact eshop for more information.","status_id":2}

Platba nebola stále prijatá, odpočítavanie stále aktívne beží:
{"error":0,"error_msg":"","status_msg":"Waiting for payment.","status_id":4}

Platba nebola prijatá na daný iframe id:
{"error":0,"error_msg":"","status_msg":"Payment not received.","status_id":5}

Iframe id neexistuje, prosím zavolajte API funkciu – KROK 1:

{"error":0,"error_msg":"","status_msg":"Iframe id does not exist!","status_id":6}

POPIS POLÍ PRE ESHOP PLUGINY

Pre Eshopy je nutné udržiavať v konfiguračnom súbore následovné parametre viditeľné pre administrátorskú rolu v platobnej časti.

Title : BTC Payment / LTC payment / atď. Podľa typu meny - Dropdown box alebo Staticky popis

Enabled: yes/no - Dropdown box

APIKEY: Varchar 36

SECKEY: TEXT <65,535 characters

FIAT Currency: dropdown box statické hodnoty - EUR, USD, GBP, JPY, CNY, AUD, CAD, AED, CZK

Payment timeout (min): Dropdown box statická hodnota integer <120 (napr. 5,10,15,30,60)

Wait confirmation : dropdown yes/no

Use proxy: dropdown yes/no

Proxy server: Varchar 60

Proxy port: Integer <10

Príklad z Magento Eshop

CryptoDiggers CDPay | CryptoDiggers ATM | CryptoDiggers Plugins Ecommerce | CryptoDiggers Vending Machines