

CardPay Direct API - dokumentácia pre obchodníka

- [Google Pay Direct API](#)
- [Apple Pay Direct API](#)
- [Device token flow - CRYPTOGRAM_3DS](#)
- [3D Secure flow - PAN_ONLY](#)
- [Vykonanie platby](#)
 - [API URL](#)
 - [Parametre požiadavky](#)
 - [Parametre odpovede](#)
- [Zistenie stavu platby](#)
 - [API URL](#)
- [Dokončenie platby \(3D Secure flow\)](#)

Google Pay Direct API

Pri implementácii Google Pay Direct API je potrebné riadiť sa pokynmi v dokumentácii na Google Developers.

[Google Pay API](#) | [Google Developers](#) - <https://developers.google.com/pay/api>

[Overview](#) | [Google Pay API for Android](#) | [Google Developers](#) - <https://developers.google.com/pay/api/android/overview>

[Overview](#) | [Google Pay API](#) | [Google Developers](#) - <https://developers.google.com/pay/api/web/overview>

Z dostupných poskytovateľov je potrebné použiť konfiguráciu pre **Tatra banka (CardPay)**.

gateway - "tatrabanka"

gatewayMerchantId - Bankou pridelený identifikátor obchodníka, MID

Apple Pay Direct API

Pri implementácii Apple Pay Direct API je potrebné riadiť sa pokynmi v dokumentácii Apple Developer.

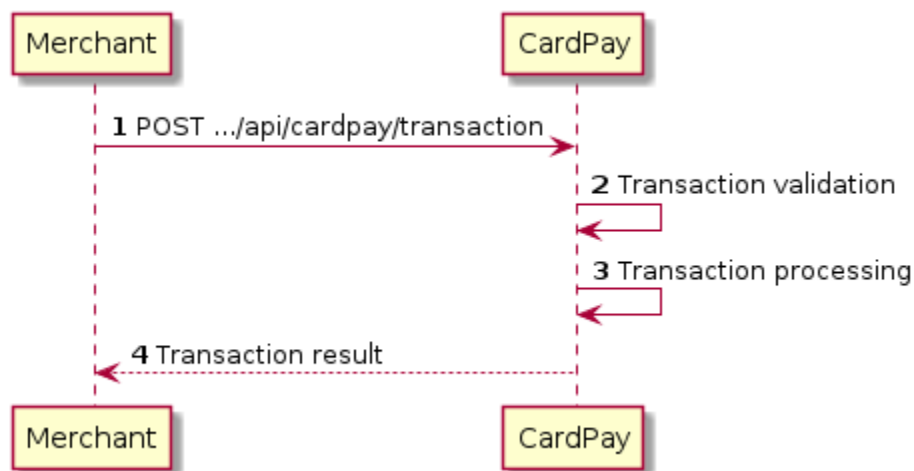
https://developer.apple.com/documentation/passkit/apple_pay

https://developer.apple.com/documentation/passkit/apple_pay/setting_up_apple_pay

Pri vytváraní Payment Processing Certificate je potrebné použiť CSR dodané Tatra bankou.

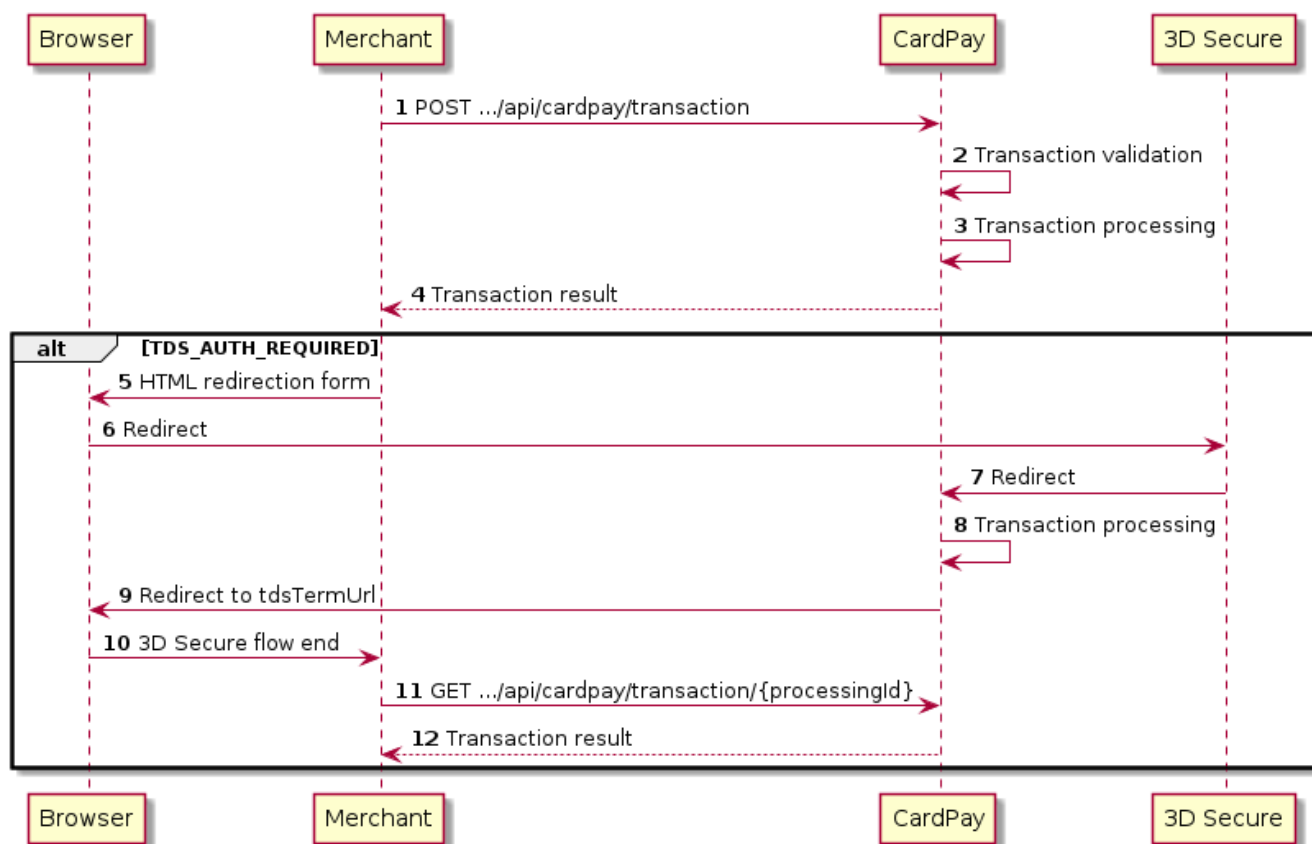
Device token flow - CRYPTOGRAM_3DS

Platí pre Google Pay, Apple Pay



3D Secure flow - PAN_ONLY

Platí pre Google Pay



Vykonanie platby

Po získaní tokenu z Google Pay API, resp. Apple Pay API je potrebné token odoslať spolu s ďalšími údajmi o platbe na platobnú bránu CardPay. Telo požiadavky je v JSON formáte.

API URL

POST <https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/api/cardpay/transaction>

Parametre požiadavky

Názov parametra	Popis	Validácie a obmedzenia
merchantId *	Bankou pridelený identifikátor obchodníka, MID	RegExp: <code>^\d{3,5}\$</code>
amount *	Suma v najmenších jednotkách zvolenej meny <i>Napr. pre 1.00 EUR sa posiela hodnota 100.</i>	Minimálna hodnota 1 a maximálna hodnota 99 999 999 999.
currency *	Číselný kód meny podľa ISO 4217	RegExp: <code>^\d{3}\$</code>
variableSymbol	Variabilný symbol	RegExp: <code>^\d{1,10}\$</code> Práve jedno z polí variableSymbol , e2eReference musí byť vyplnené.

e2eReference	Referencia platiteľa	RegExp: <code>^[a-zA-Z\\d/?.,:()'+-]{1,35}\$</code> Práve jedno z polí variableSymbol , e2eReference musí byť vyplnené.				
clientIpAddress *	IP adresa klienta vo formáte IPv4 alebo IPv6	Minimálne 1 a maximálne 45 znakov.				
clientName *	Meno alebo e-mailová adresa klienta	RegExp: <code>^[a-zA-Z\\d.@_ -]{1,64}\$</code>				
timestamp *	Časový odtlačok požiadavky vo formáte ddMMyyyyHHmmss	RegExp: <code>^\\d{14}\$</code> Musí byť v rozsahu UTC +/- 1 hodina.				
googlePayToken	Hodnota <code>paymentData.paymentMethodData.tokenizationData.token</code>	Práve jedno z polí googlePayToken , applePay musí byť vyplnené.				
applePay	<table><tr><th>Názov parametra</th><th>Popis</th></tr><tr><td>token *</td><td>Hodnota z <code>PKPayment.token.paymentData</code> (https://developer.apple.com/documentation/passkit/pkpaymenttoken/1617000-paymentdata) ako JSON objekt. Príklad požiadavky: <pre>{ ... "applePay": { "token": { "header": { "ephemeralPublicKey": string, "publicKeyHash": string, "transactionId": string }, "data": string, "signature": string, "version": "EC_v1" } }, ... }</pre></td></tr></table>		Názov parametra	Popis	token *	Hodnota z <code>PKPayment.token.paymentData</code> (https://developer.apple.com/documentation/passkit/pkpaymenttoken/1617000-paymentdata) ako JSON objekt. Príklad požiadavky: <pre>{ ... "applePay": { "token": { "header": { "ephemeralPublicKey": string, "publicKeyHash": string, "transactionId": string }, "data": string, "signature": string, "version": "EC_v1" } }, ... }</pre>
Názov parametra	Popis					
token *	Hodnota z <code>PKPayment.token.paymentData</code> (https://developer.apple.com/documentation/passkit/pkpaymenttoken/1617000-paymentdata) ako JSON objekt. Príklad požiadavky: <pre>{ ... "applePay": { "token": { "header": { "ephemeralPublicKey": string, "publicKeyHash": string, "transactionId": string }, "data": string, "signature": string, "version": "EC_v1" } }, ... }</pre>					
preAuthorization	Príznak, či je transakcia preautORIZÁCIA.	Boolean				
tdsTermUrl	URL, na ktorú má prísť presmerovanie po dokončení 3D Secure overenia. Ak nie je odoslané a je vyžadované 3D Secure overenie, transakcia skončí v stave FAIL.	Musí byť platná URL adresa.				
tdsData	Dodatočné parametre pre 3D Secure overenie					

Názov parametra	Popis	Validácie a obmedzenia
cardholder	Meno držiteľa karty	RegExp: <code>^[0-9a-zA-Z. @_-] {2,45}\$</code>
email	Emailová adresa	RegExp: <code>^[0-9a-zA-Z. @_-] {1,254}\$</code>
mobilePhone	Telefónne číslo Vo formáte {Predvoľba}-{Telefónne číslo}	RegExp: <code>^\d{1,3}-\d{1,15}\$</code>
billingCity	Fakturačná adresa - mesto	RegExp: <code>^[0-9a-zA-Z. @_-] {1,50}\$</code>
billingCountry	Fakturačná adresa - krajina Číselný kód krajiny podľa ISO 3166-1	RegExp: <code>^\d{3}\$</code>
billingAddress1	Fakturačná adresa - ulica	RegExp: <code>^[0-9a-zA-Z. @_-] {1,50}\$</code>
billingAddress2	Fakturačná adresa - ulica - pokračovanie	RegExp: <code>^[0-9a-zA-Z. @_-] {1,50}\$</code>
billingZip	Fakturačná adresa - PSČ	RegExp: <code>^[0-9a-zA-Z. @_-] {1,16}\$</code>
shippingCity	Doručovací adresa - mesto	RegExp: <code>^[0-9a-zA-Z. @_-] {1,50}\$</code>
shippingCountry	Doručovací adresa - krajina Číselný kód krajiny podľa ISO 3166-1	RegExp: <code>^\d{3}\$</code>
shippingAddress1	Doručovací adresa - ulica	RegExp: <code>^[0-9a-zA-Z. @_-] {1,50}\$</code>
shippingAddress2	Doručovací adresa - ulica - pokračovanie	RegExp: <code>^[0-9a-zA-Z. @_-] {1,50}\$</code>
shippingZip	Doručovací adresa - PSČ	RegExp: <code>^[0-9a-zA-Z. @_-] {1,16}\$</code>
billingShippingMatch	Indikuje, či je doručovací adresa rovnaká ako fakturačná	

ipspData

Dodatkové parametre pre Payment Facilitator

Povinné, ak je obchodník Payment Facilitator.

Názov parametra	Popis	Validácie a obmedzenia
submerchantId	Identifikátor konečného obchodníka	RegExp: <code>^\d{1,15}\$</code>
name	Názov	RegExp: <code>^[0-9a-zA-Z. @_-] {1,25}\$</code>
location	Lokalita	RegExp: <code>^[0-9a-zA-Z. @_-] {1,13}\$</code>
country	Krajina Číselný kód krajiny podľa ISO 3166-2	RegExp: <code>^[A-Z]{2}\$</code>



Každá požiadavka smerujúca na API platobnej brány CardPay musí obsahovať HTTP hlavičky **Authorization** a **X-Merchant-Id**. Hlavička **Authorization** obsahuje podpis požiadavky. Hlavička **X-Merchant-Id** obsahuje bankou pridelený identifikátor obchodníka.

Príklad požiadavky

```
POST /cgi-bin/e-commerce/start/api/cardpay/transaction HTTP/1.1
X-Merchant-Id: 6855
Authorization: HMAC=3045...d43f
```

```
{
  "merchantId": "6855",
  "amount": 42,
  "currency": "978",
  "variableSymbol": "123",
  "clientIpAddress": "127.0.0.1",
  "clientName": "mail@example.org",
  "timestamp": "12102021094831",
  "googlePayToken": "...",
  "tdsTermUrl": "https://localhost:4200/tds.html"
}
```



Autorizačná hlavička

Odpisuje sa celé telo požiadavky. Z tela požiadavky (`requestBody`) sa bez akejkoľvek modifikácie vygeneruje hašovaný autentifikačný kód (HMAC) použitím kryptografickej funkcie SHA-256 a 64-bajtového bezpečnostného kľúča (`key`), ktorý je zapísaný v hexadecimálnom tvare (128 znakov).

`HMAC_SHA256(key, requestBody) = hmac`

Výsledok sa vloží do HTTP hlavičky **Authorization** vo formáte `HMAC=hmac`

Po zvalidovaní požiadavky a realizácii transakcie obdrží obchodník v odpovedi výsledok transakcie. Stav transakcie môže byť finálny (`OK`, `FAIL`) alebo môže signalizovať potrebu overenia pomocou 3D Secure (`TDS_AUTH_REQUIRED`).

Parametre odpovede

Názov parametra	Popis	Validácie a obmedzenia
processingId *	API identifikátor transakcie	
status *	Stav transakcie OK - transakcia bola úspešne vykonaná FAIL - transakcia zlyhala TDS_AUTH_REQUIRED - vyžaduje sa overenie v 3D Secure	
transactionId	Identifikátor transakcie	Iba pre status OK a FAIL
transactionData	Údaje o výsledku transakcie	Iba pre status OK a FAIL

	Názov parametra	Popis	Validácie a obmedzenia
	responseCode *	kód chyby (response code) dvojnakový kód – kód z výsledku autorizácie, ak transakcia bola odoslaná na autorizáciu, alebo: FDS – ak transakcia zlyhala pri overení vo Fraud detection systéme; TDS – ak transakcia zlyhala pri 3D Secure overení; SYS – ak pri spracovaní transakcie nastala systémová chyba.	RegExp: <code>^[0-9A-Z]{2,3}\$</code>
	authorizationCode	Autorizačný kód	RegExp: <code>^[0-9A-Z]{6}\$</code>
tdsRedirectionFormHtml	HTML formulár, ktorý zabezpečí presmerovanie do 3D Secure procesu.		Iba pre status TDS_AUTH_REQUIRED

Príklad odpovede (finálny stav)

```
HTTP/1.1 201
Authorization: HMAC=4ebd...3337, ECDSA=30450220...5b2ed43f, ECDSA_KEY=1

{
  "processingId": 1117,
  "status": "OK",
  "transactionId": 45874531,
  "transactionData": {
    "authorizationCode": "MH1234",
    "responseCode": "00"
  }
}
```

Príklad odpovede (potrebné overenie v 3D Secure)

```
HTTP/1.1 201
Authorization: HMAC=4ebd...3337, ECDSA=30450220...5b2ed43f, ECDSA_KEY=1

{
  "processingId": 1117,
  "status": "TDS_AUTH_REQUIRED",
  "tdsRedirectionFormHtml": "<!DOCTYPE html><html lang='en'><head><meta charset='UTF-8'><title>3D Secure Processing</title></head><body><form action='https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/api/form/cardpay/transaction/tds' method='POST' name='redirectionForm'><input type='hidden' name='processingId' value='1117'><input type='hidden' name='timestamp' value='12102021094831'><input type='hidden' name='signature' value='...'><noscript><button type='submit'>Continue</button></noscript><script>document.forms.redirectionForm.submit();</script></form></body></html>"
}
```



Autorizačná hlavička

Podpisuje sa celé telo odepovede. Z tela odpovede (`responseBody`) sa bez akejkoľvek modifikácie vygeneruje hašovaný autentifikačný kód (HMAC) použitím kryptografickej funkcie SHA-256 a 64-bajtového bezpečnostného kľúča (`key`), ktorý je zapísaný v hexadecimálnom tvare (128 znakov).

```
HMAC_SHA256(key, responseBody) = hmac
```

Výsledok sa vloží do HTTP hlavičky **Authorization** vo formáte `HMAC=hmac, ECDSA=ecdsa, ECDSA_KEY=ecdsa_key`



Obchodník je povinný overiť si HMAC a aj ECDSA podpis v odpovedi.

Zistenie stavu platby

API URL

GET <https://moja.tatrabanka.sk/cgi-bin/e-commerce/start/api/cardpay/transaction/{processingId}>

Príklad požiadavky

```
GET /cgi-bin/e-commerce/start/api/cardpay/transaction/1117 HTTP/1.1
X-Merchant-Id: 6855
X-Timestamp: 12102021094831
Authorization: HMAC=3045...d43f
```



Autorizačná hlavička

Podpisuje sa reťazec (`stringToSign`) hodnôt z hlavičiek **X-Merchant-Id**, **X-Timestamp** a z parametra **processingId**, ktorý je súčasťou URL. Z tohto reťazca sa vygeneruje hašovaný autentifikačný kód (HMAC) použitím kryptografickej funkcie SHA-256 a 64-bajtového bezpečnostného kľúča (`key`), ktorý je zapísaný v hexadecimálnom tvare (128 znakov).

```
stringToSign = VALUE(X-Merchant-Id) + ";" + VALUE(X-Timestamp) + ";" + processingId
HMAC_SHA256(key, stringToSign) = hmac
```

Výsledok sa vloží do HTTP hlavičky **Authorization** vo formáte **HMAC=hmac**

Príklad odpovede (finálny stav)

```
HTTP/1.1 200
Authorization: HMAC=4ebd...3337, ECDSA=30450220...5b2ed43f, ECDSA_KEY=1

{
  "processingId": 1117,
  "status": "OK",
  "transactionId": 45874531,
  "transactionData": {
    "authorizationCode": "MH1234",
    "responseCode": "00"
  }
}
```



Autorizačná hlavička

Podpisuje sa celé telo odepovede. Z tela odpovede (`responseBody`) sa bez akejkoľvek modifikácie vygeneruje hašovaný autentifikačný kód (HMAC) použitím kryptografickej funkcie SHA-256 a 64-bajtového bezpečnostného kľúča (`key`), ktorý je zapísaný v hexadecimálnom tvare (128 znakov).

```
HMAC_SHA256(key, responseBody) = hmac
```

Výsledok sa vloží do HTTP hlavičky **Authorization** vo formáte **HMAC=hmac, ECDSA=ecdsa, ECDSA_KEY=ecdsa_key**



Obchodník je povinný overiť si HMAC a aj ECDSA podpis v odpovedi.

Dokončenie platby (3D Secure flow)

V prípade, ak sa transakcia dostane do stavu `TDS_AUTH_REQUIRED`, je potrebné vykonať dodatočné overenie v programe 3D Secure. S týmto overením pomôže automaticky generovaný HTML formulár obsiahnutý v poli `tdsRedirectionFormHtml`. Formulár je potrebné v novom okne zobraziť klientovi a automaticky sa vykoná presmerovanie do 3D Secure procesu. Po dokončení overenia sa aktualizuje stav transakcie a dôjde k presmerovaniu na `tdsTermUrl`. Po tomto presmerovaní musí obchodník odoslať požiadavku na [Zistenie stavu platby](#), aby zistil výsledok transakcie.